Building World Class Cyber Security Training Facilities

Experience in researching and building a cyber range -NCR

Muhammad Mudassar Yamin

Rome wasn’t built in a day!

but it was burnt to the ground in only six

Motivation

Cyber attacks costs and impact

IBM

Key stats

Investing now can sa

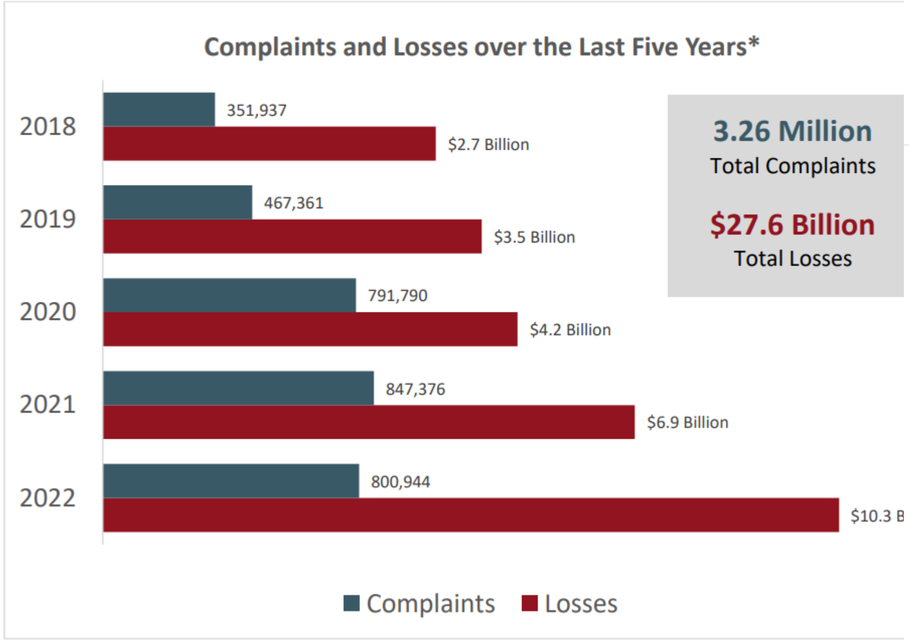
USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

IC3 COMPLAINT STATISTICS

LAST FIVE YEARS

Over the last five years, the IC3 has received an average of 652,000 complaints per year. These compl address a wide array of Internet scams affecting victims across the globe.[3]



Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

November 18, 2020 11:03 ET| Source: INTRUSION Inc. Follow

PLANO, Texas, Nov. 18, 2020 (GLOBE NEWSWIRE) -- Cybersecurity Ventures predicts global cybercrime costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This prediction is part of a special report conducted by Cybersecurity Ventures and sponsored by **INTRUSION**, Inc. (NASDAQ: INTZ).

https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf


Some men just want to watch the world burn!

Motivation

Small and medium Enterprises are targets

UpCity

Top 3 Reasons Eve Care Abo

By: Mario DiM

the news right? Here are 3
care about cybersecurity a
protect your small business

Hackers Love Small Bu

The facts are that the majo
smaller companies and the
they do, they don't make th

Easy Prey

Small businesses often neg
due to budgetary concerns
unaware, don't know where

Out Of Business

If (when) a small business i
chance (over 50%) that the
from lost productivity, repu
can be too great.

UpCity

One alternative to using a text message would be apps on your phone (Google Authenticator and Authy are popular options) that generate unique codes that take the place of the text message.

The People Problem

Even if your IT systems are protected with adequate cybersecurity measures, there is one gaping hole in most security plans and hackers love to exploit this. Your employees. They are easy to trick into clicking something they shouldn't or even providing information over the phone or in-person that is confidential.

What To Do

Train your employees using a regular system of security awareness training. The plan should also include a way to test phish (sending them fake phishing emails to see who your "clickers" are) your people. Good systems of training are fun, easy to learn, and constantly updated over time to adapt to current trends. KnowBe4 is a great place to start and offers all the above and more to train your people.

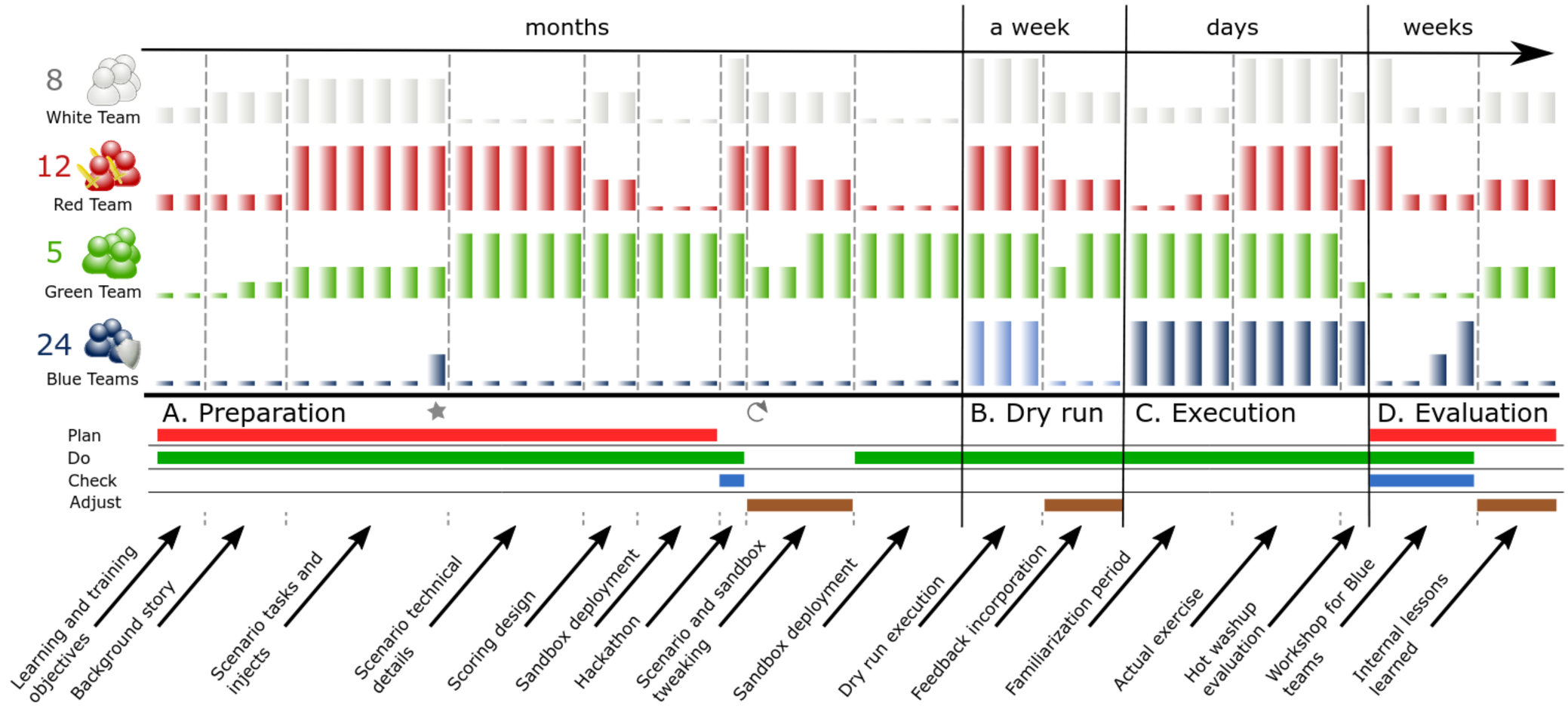
https://upcity.com/experts/top-reasons-small-businesses-should-care-about-cybersecurity/


We need to train people to fight cyber arsonist

Physical Environment for Capabilities Training and Testing

Motivation

Cyber security training and exercises are costly



Vykopal, Jan, et al. "Lessons learned from complex hands-on defence exercises in a cyber range." *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2017.

What is a Cyber Range?

"A cyber range is a platform for the development, delivery and use of interactive simulation/emulation environments. A simulation/emulation environment is a **representation of an organisation**'s ICT, OT, mobile and physical systems, applications and infrastructures, including the **simulation of attacks, users and their activities** and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation/emulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases."

European Cyber Security Organisation (ECSO), "Understanding Cyber Ranges from Hype to Reality" (White Paper) rel. 30-March 2020.

What is a Cyber Range?

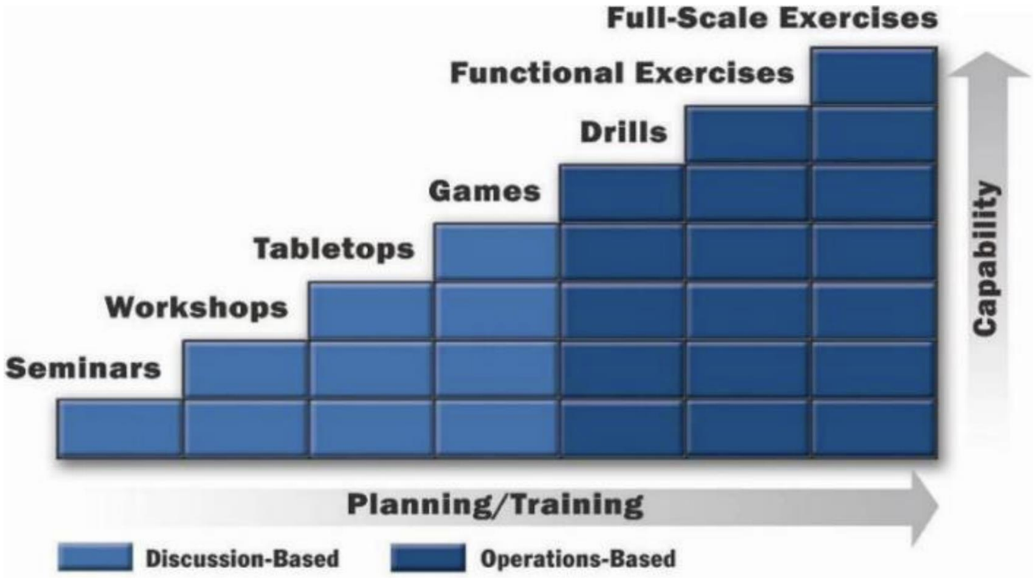
Cyber range use cases

- Competence building
- Security education
- Competence assessment
- Security testing
- Security research
- Development of cyber capabilities and resilience

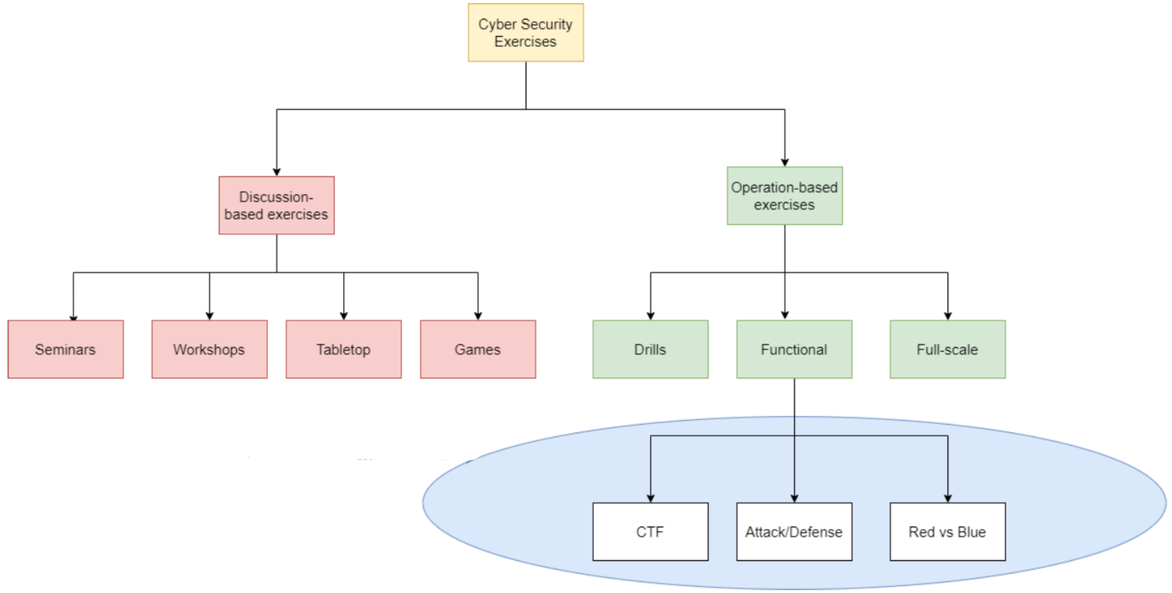
European Cyber Security Organisation (ECSO), "Understanding Cyber Ranges from Hype to Reality" (White Paper) rel. 30-March 2020.

Cyber Security Exercises

Types of cyber security exercises

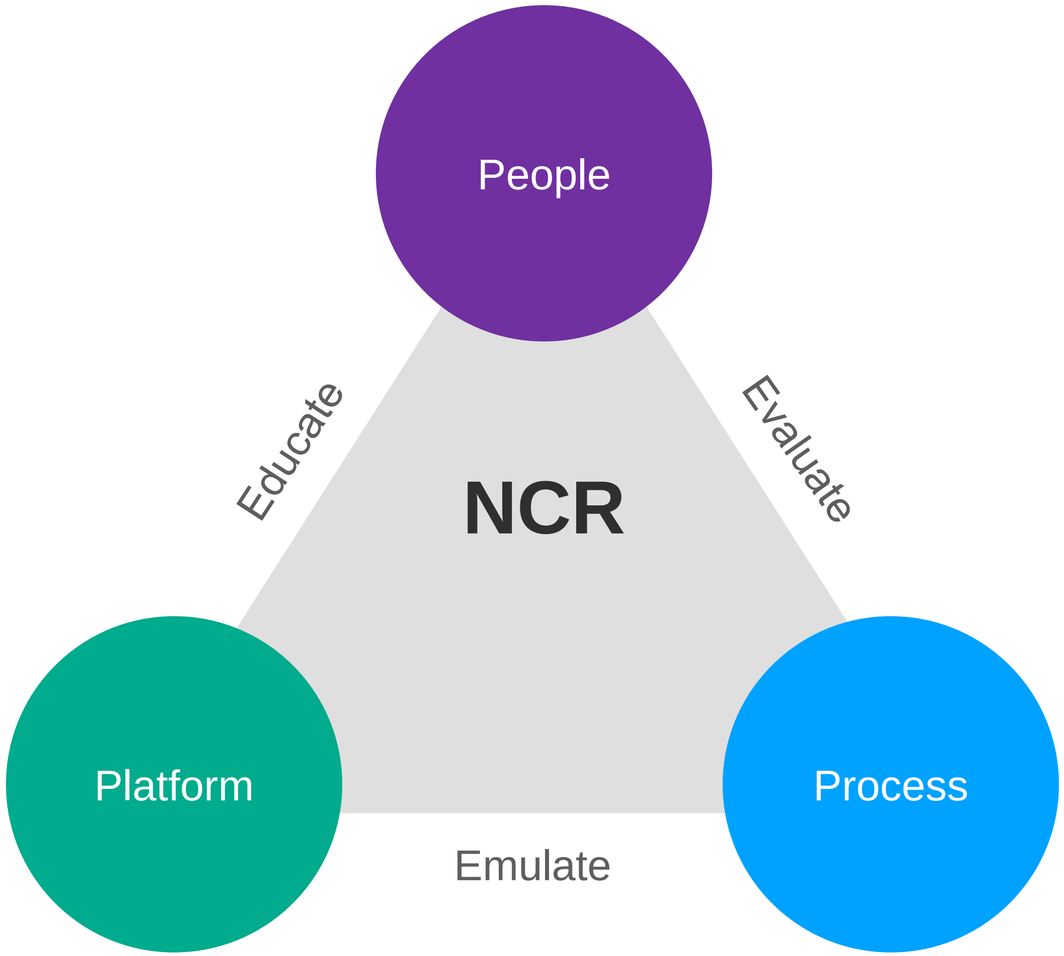


Introduction to Cyber Exercises, National Cyber Security, Division Cyber Exercise Program, DHS, 2003.



Yamin, M. M. (2022). Modelling and analyzing attack-defense scenarios for cyber-ranges.

The Norwegian Cyber Range



People

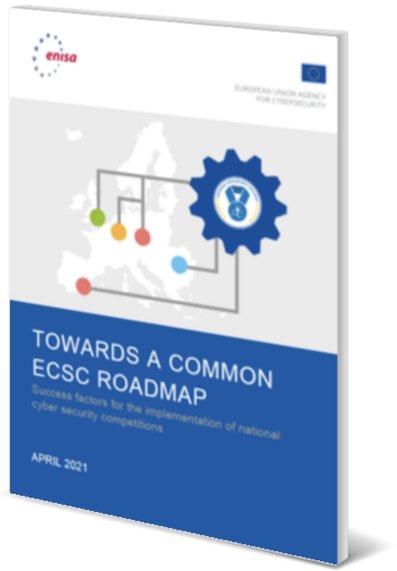
People

Addressing cyber security skill shortage through CTF competitions

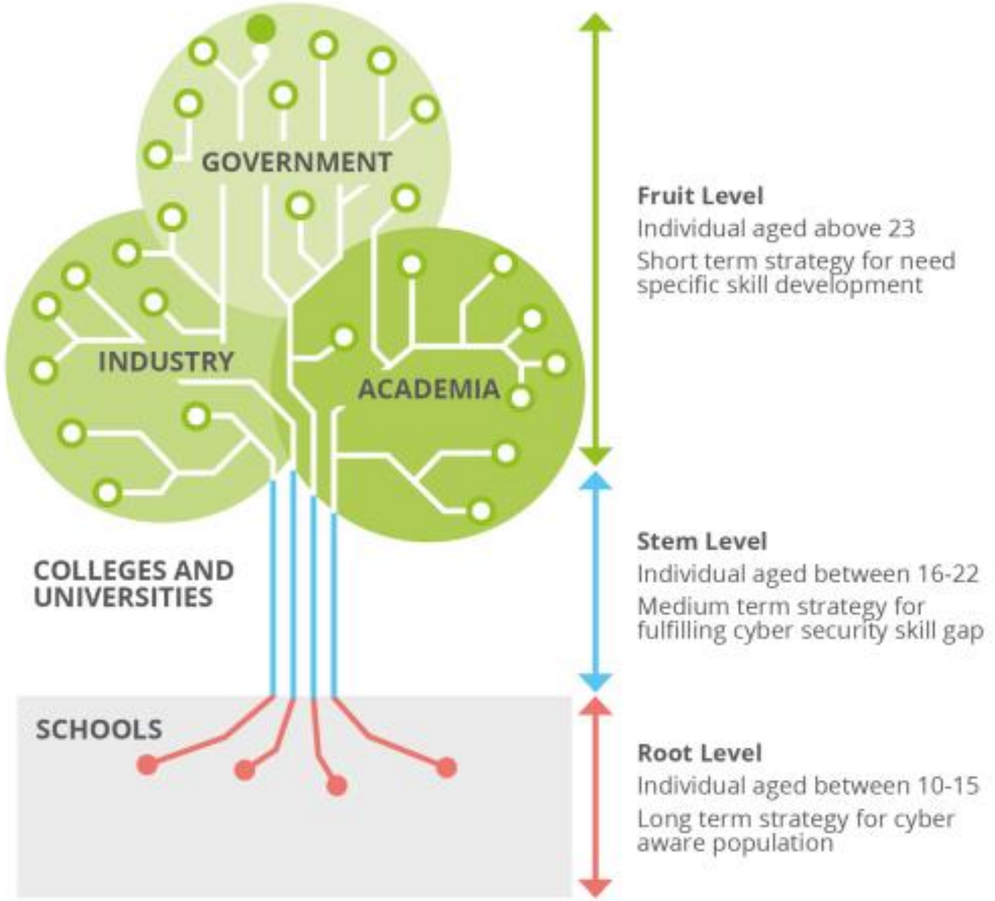
Towards a Common ECSC roadmap

This report aimed to identify the key factors enabling the success of a national cybersecurity competition and to give a snapshot of the current situation in the EU and ECSC partner countries. To do that, we conducted a dozen of interviews with national and EU experts, searched and reviewed the relevant scientific literature and collected data on these key enabling factors with a survey, which was filled by 90% of the countries attending the ECSC. This was done to provide preliminary insights and a discussion platform to determine a common ECSC roadmap.

Published April 12, 2021
Language English



Download
PDF document, 1.84 MB



https://www.enisa.europa.eu/publications/towards-a-common-ecsc-roadmap

People

Nourishing active CTF communities in Gjovik and Trondhiem

System Security Research Group
Playground

S2G
System Security | Research group

PLAYGROUND

General

We invite all students from NTNU to take part in our regular S2G Playground events:

- S2G CTF (Capture The Flag events),
- S2G Hackathon,
- S2G ST (Security Testing).

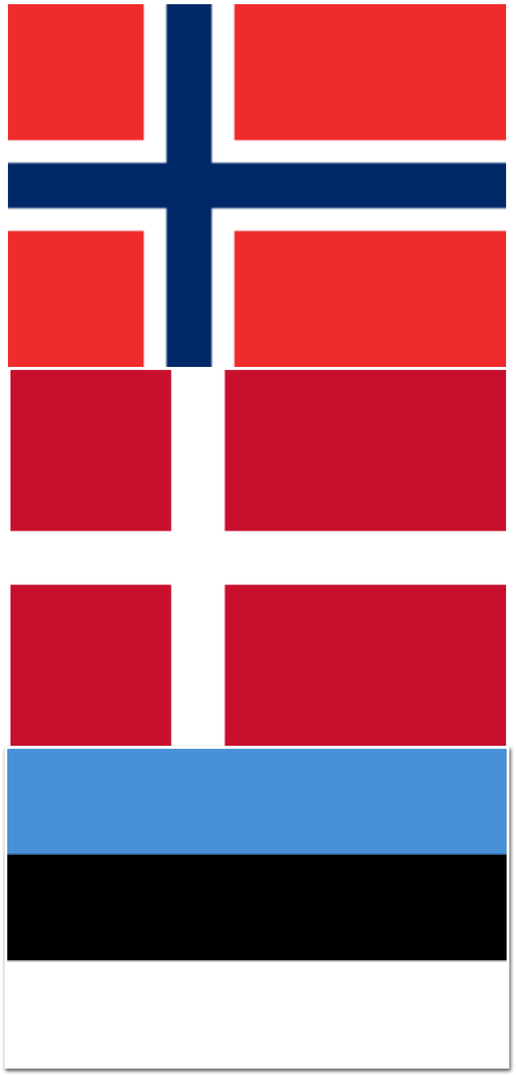
Next Playground

CTF on 16 of November from 16:15 online in the Teams/Discord channels and physically in Room S410 Register here if coming on campus

Join S2G Playground Event

People

Responsible for selecting and training National Cyber security team of Norway

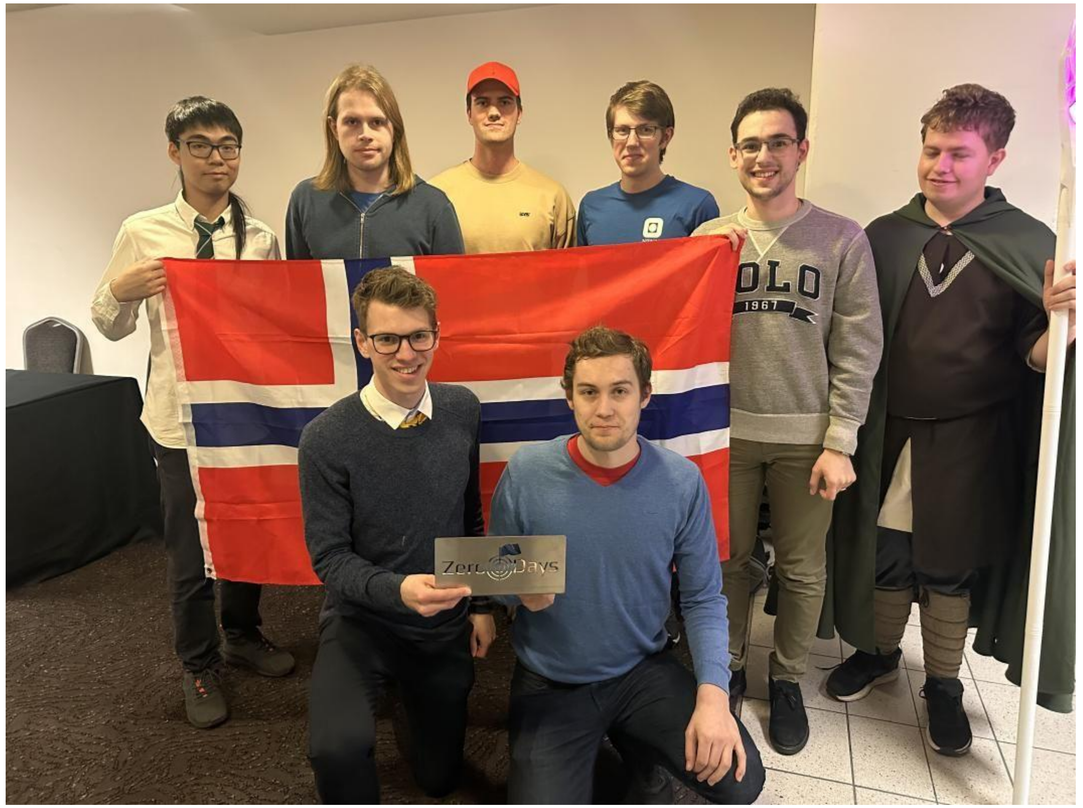


People

Dream:Nordic Baltic Cyber Summer Camp

People

Participating in different national and International competitions



Process

Process

Cyber Security Exercise Lifecycle

ELSEVIER

Computers & Security
Volume 116, May 2022, 102635

TC 11 Briefing Papers

Modeling and executing cyber security exercise scenarios in cyber ranges

Muhammad Mudassar Yamin, Basel Katt

Show more

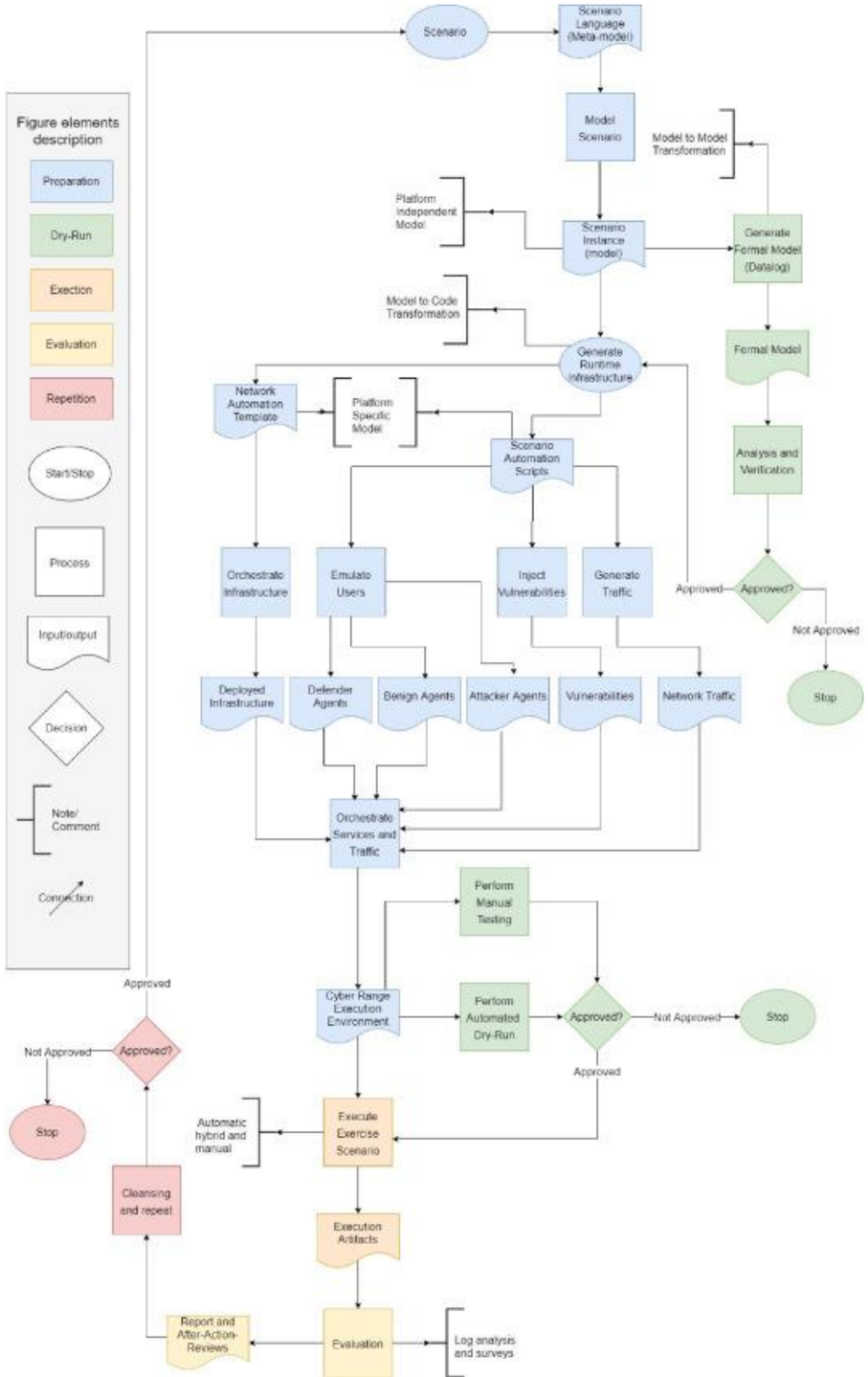
+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2022.102635

Get rights and content

Abstract

The skill shortage in global cybersecurity is a well-known problem; to overcome this issue, cyber ranges have been developed. These ranges provide a platform for conducting cybersecurity exercises; however, conducting such exercises is a complex process because they involve people with different skill sets for the scenario modeling, infrastructure preparation, dry run, execution, and evaluation. This process is very complex and inefficient in terms of time and resources. Moreover, the exercise infrastructure created in current cyber ranges does not reflect the dynamic environment of real-world systems and does not provide adaptability for changing requirements. To tackle these issues, we developed a system that can automate many tasks of the cybersecurity exercise life cycle. We used model-driven approaches to (1) model the roles of the different teams present in the cybersecurity exercises and (2) generate automation artifacts to execute their functions efficiently



Process

ASCERT:AI-Based Scenario Management for Cyber Range Training

Scenario Design Frontend
supports skill-centered scenario design on and across strategic, tactical and operational levels

Graphical representation in *Attack-Defence Trees*

AI-Based Scenario Planner and Reasoner
computes relevant plays through a scenario and their skill-centered goal metrics

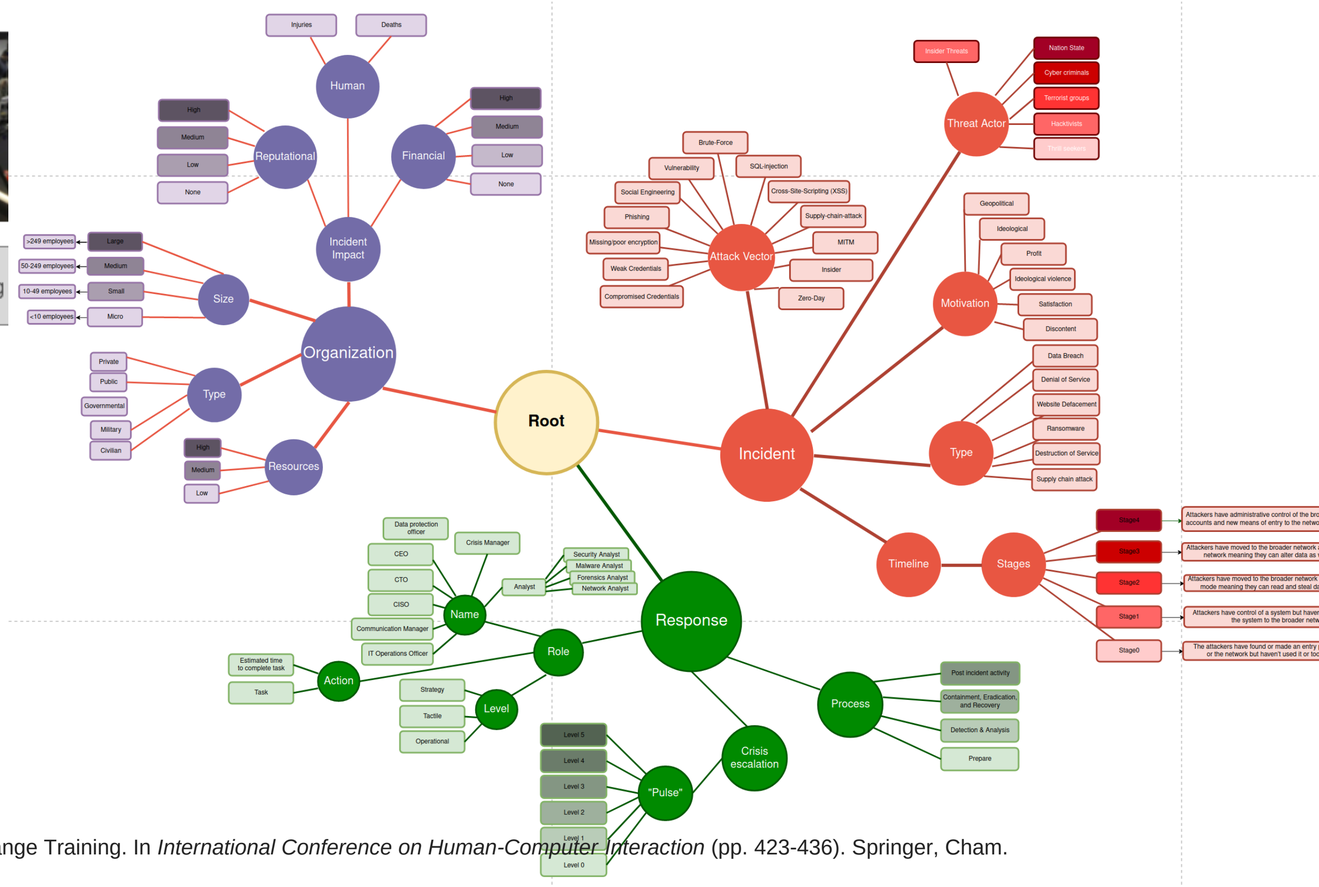
Logical representation in *Formal Argumentation Theory* and *Answer Set Programming*

Digital Scenario
events
environment
metrics

AI-Based Event Controller
executes scenario and updates goals by generating events based on user actions during execution

AI-Based Infrastructure Orchestration Controller
generates and updates emulated environment based on scenario and user actions during scenario execution

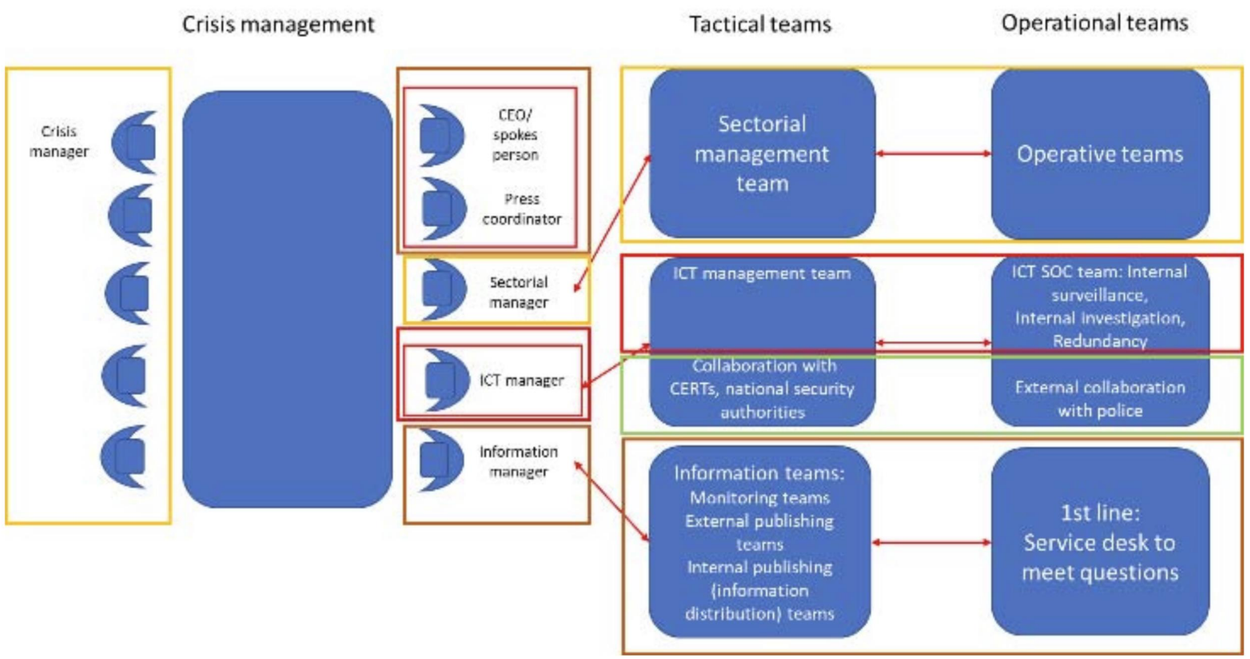
Emulated System
renders the scenario during execution

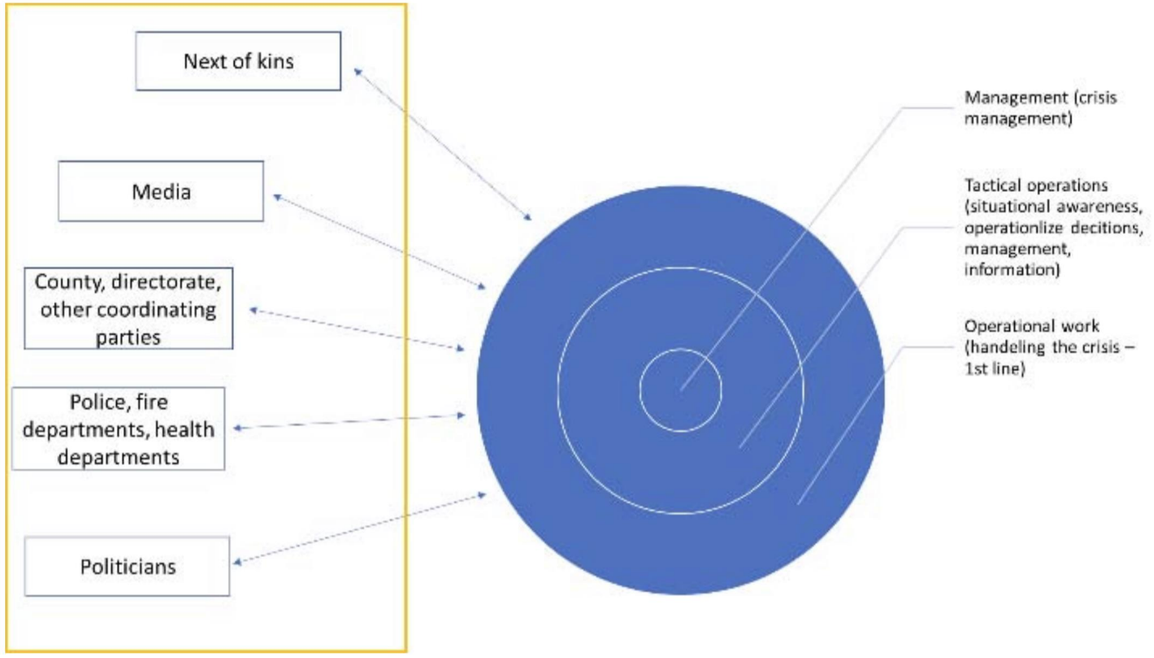


Hannay, J. E., Stolpe, A., & Yamin, M. M. (2021, July). Toward AI-Based Scenario Management for Cyber Range Training. In *International Conference on Human-Computer Interaction* (pp. 423-436). Springer, Cham.

Process

Cyber Crisis Management





Østby, G., Lovell, K. N., & Katt, B. (2019, December). EXCON teams in cyber security training. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 14-19). IEEE.

Platform

Platform

Cyber range ontology

ELSEVIER

Computers & Security
Volume 88, January 2020, 101636

Cyber ranges and security testbeds: Scenarios, functions, tools and architecture

Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos

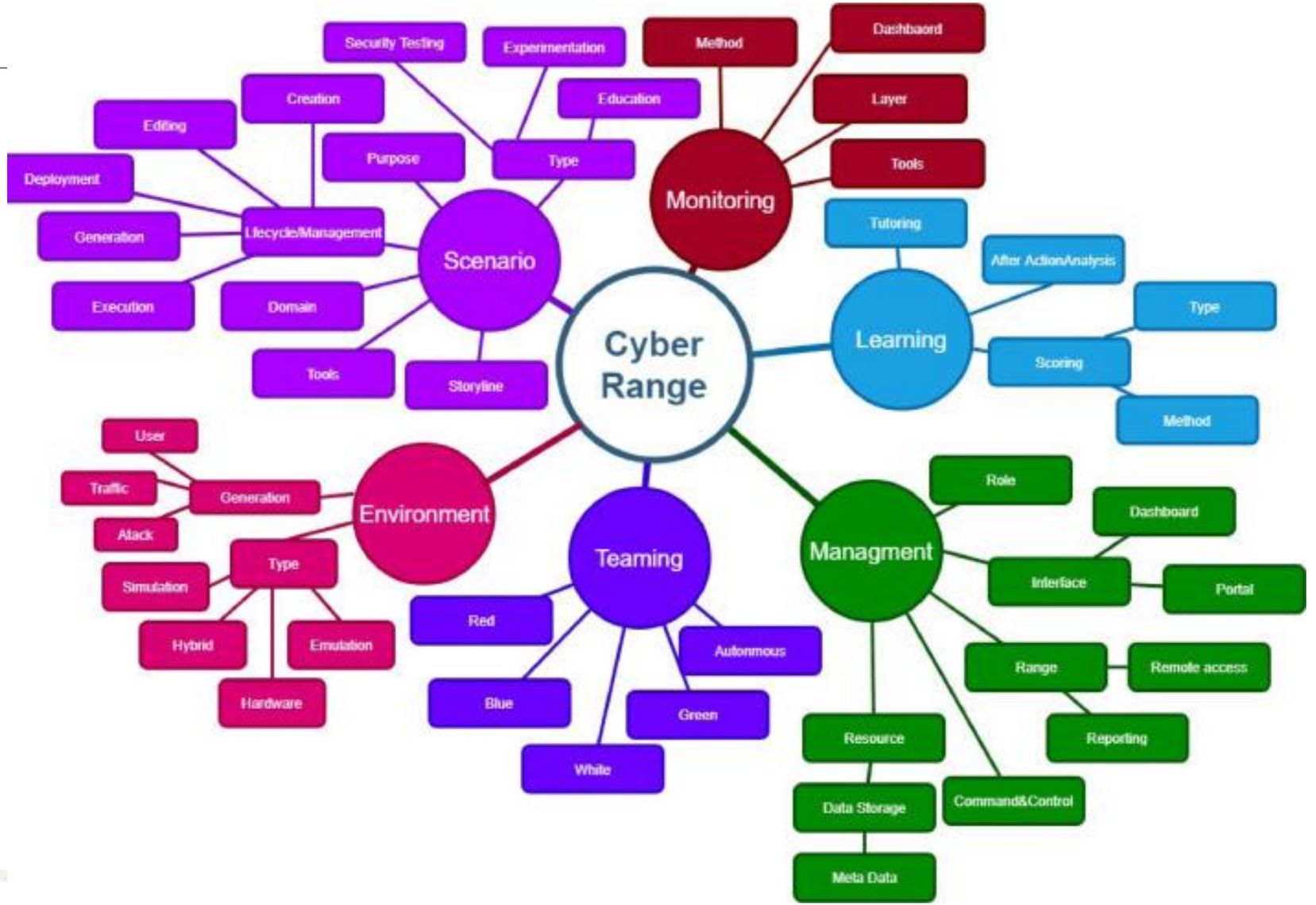
Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2019.101636 Get rights and content

Abstract

The first line of defense against cyber threats and cyber crimes is to be aware and get ready, e.g., through cyber security training. Training can have two forms, the first is directed towards security professionals and aims at improving understanding of the latest threats and increasing skill levels in defending and mitigating against them. The second form of training, which used to attract less attention, aims at increasing cyber security awareness among non-security professionals and the general public. Conducting such training programs requires dedicated testbeds and infrastructures that help realizing and executing the training scenarios and provide a playground for the trainees. A *cyber range* is an environment that aims at providing such testbeds. The purpose of this paper is to study the concept of a cyber range, and provide a systematic literature review that covers unclassified cyber ranges and security testbeds. In this study we develop a taxonomy for cyber range systems and evaluate the current literature focusing on architecture and scenarios, but including



Platform

Norwegian Cyber Range Operational Exercise Orchestrator

ELSEVIER

Computers & Security
Volume 116, May 2022, 102635

TC 11 Briefing Papers

Modeling and executing cyber security exercise scenarios in cyber ranges

Muhammad Mudassar Yamin, Basel Katt

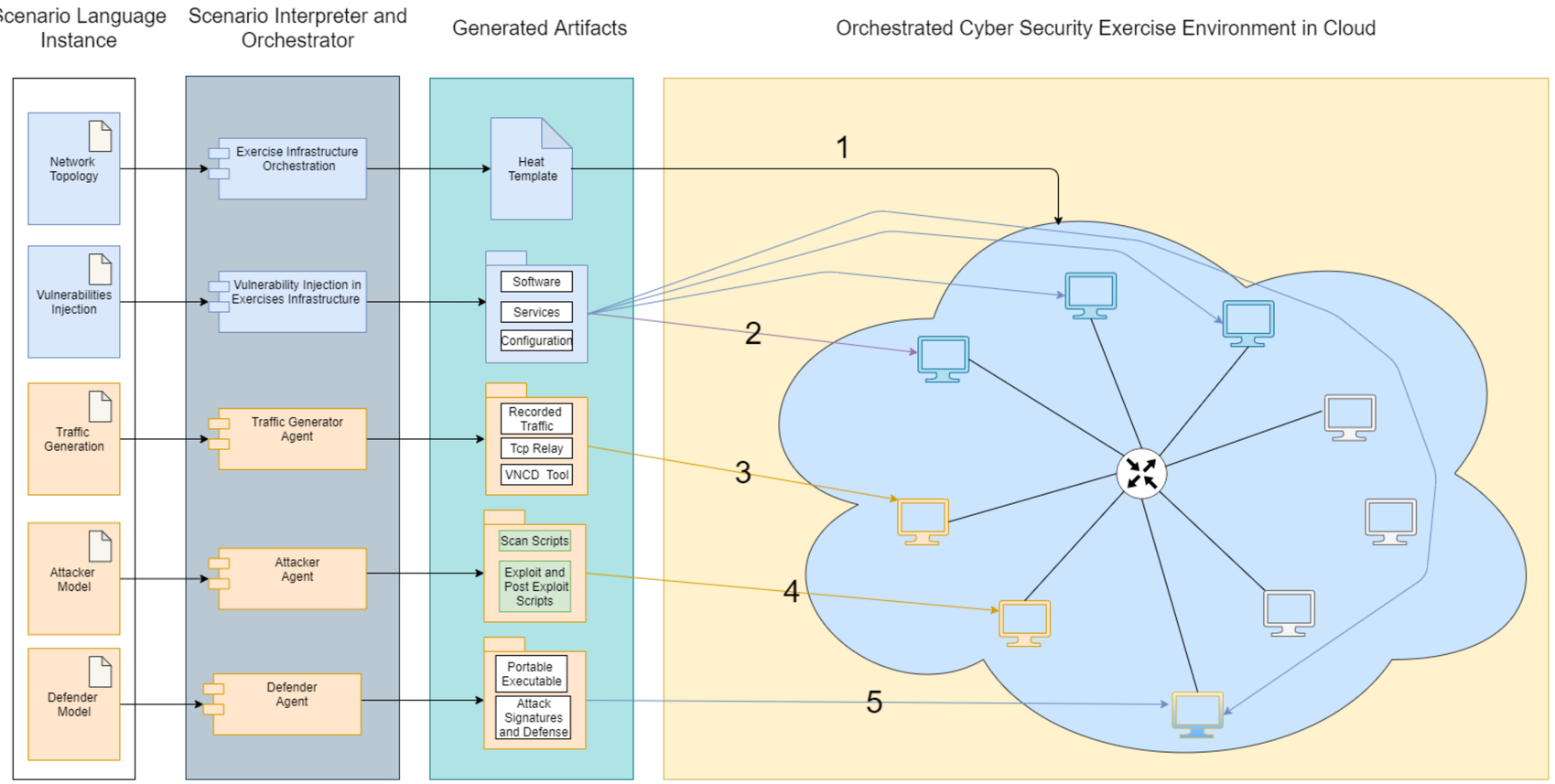
Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2022.102635 Get rights and content

Abstract

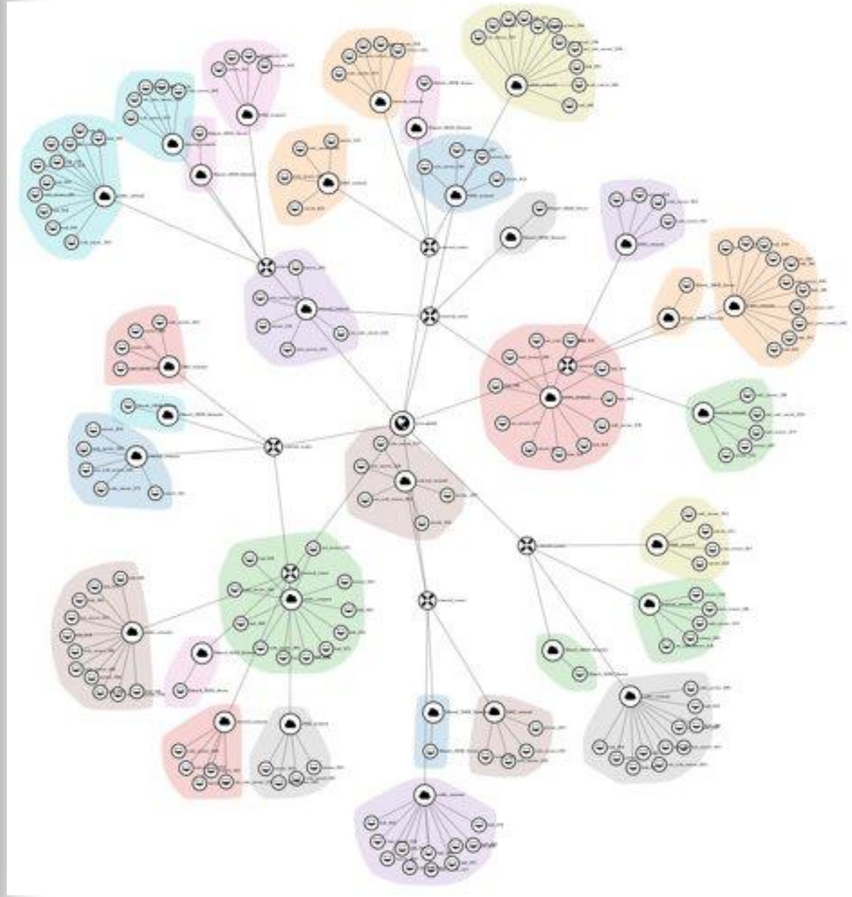
The skill shortage in global cybersecurity is a well-known problem; to overcome this issue, cyber ranges have been developed. These ranges provide a platform for conducting cybersecurity exercises; however, conducting such exercises is a complex process because they involve people with different skill sets for the scenario modeling, infrastructure preparation, dry run, execution, and evaluation. This process is very complex and inefficient in terms of time and resources. Moreover, the exercise infrastructure created in current cyber ranges does not reflect the dynamic environment of real-world systems and does not provide adaptability for changing requirements. To tackle these issues, we developed a system that can automate many tasks of the cybersecurity exercise life cycle. We used model-driven approaches to (1) model the roles of the different teams present in the cybersecurity exercises and (2) generate automation artifacts to execute their functions efficiently

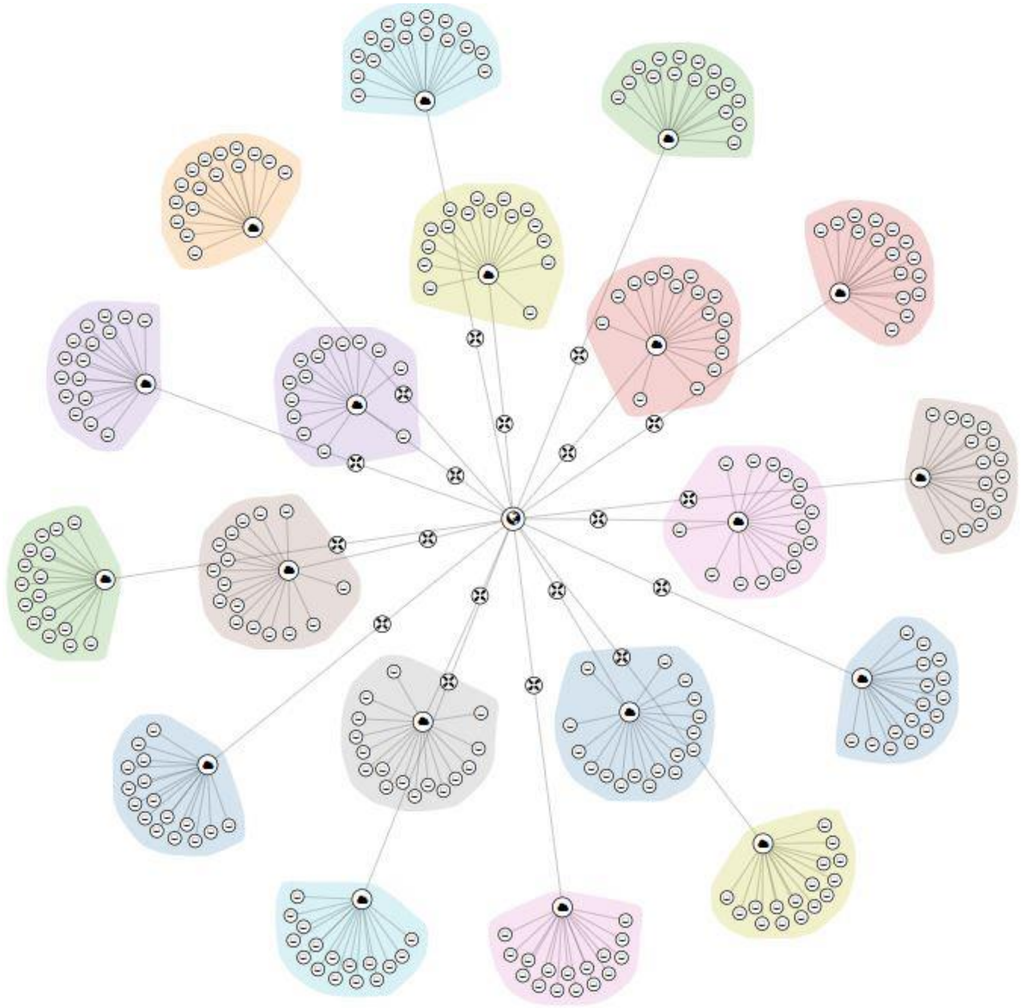


Platform

Operational Cyber Security exercises Infrastructure

```yaml
scenario:
  name: iceland
  description: iceland exercies
  start: 2022-03-16
  end: 2022-03-31
  infrastructure:
    - public_network:
        kali: 6
        server: 2
        vulnerable_server: 3
        vulnerabiltities:
          - sqli
          - xss
          - rce
          - ftp_brute_force
          - buffer_overflow
    - mz_network:
        server: 2
        vulnerable_server: 2
        vulnerabiltities:
          - sqli
          - xss
          - rce
          - ftp_brute_force
          - buffer_overflow
    - internal_network:
        server: 3
        vulnerable_server: 2
        vulnerabiltities:
          - sqli
          - xss
          - rce
          - ftp_brute_force
          - buffer_overflow
    - siem_network: true
#   - Attacker_network: true
```





Platform

Operational Cyber Security exercises Infrastructure

ELSEVIER

Computers & Security

Volume 122, November 2022, 102892

Use of cyber attack and defense agents in cyber ranges: A case study

Muhammad Mudassar Yamin, Basel Katt

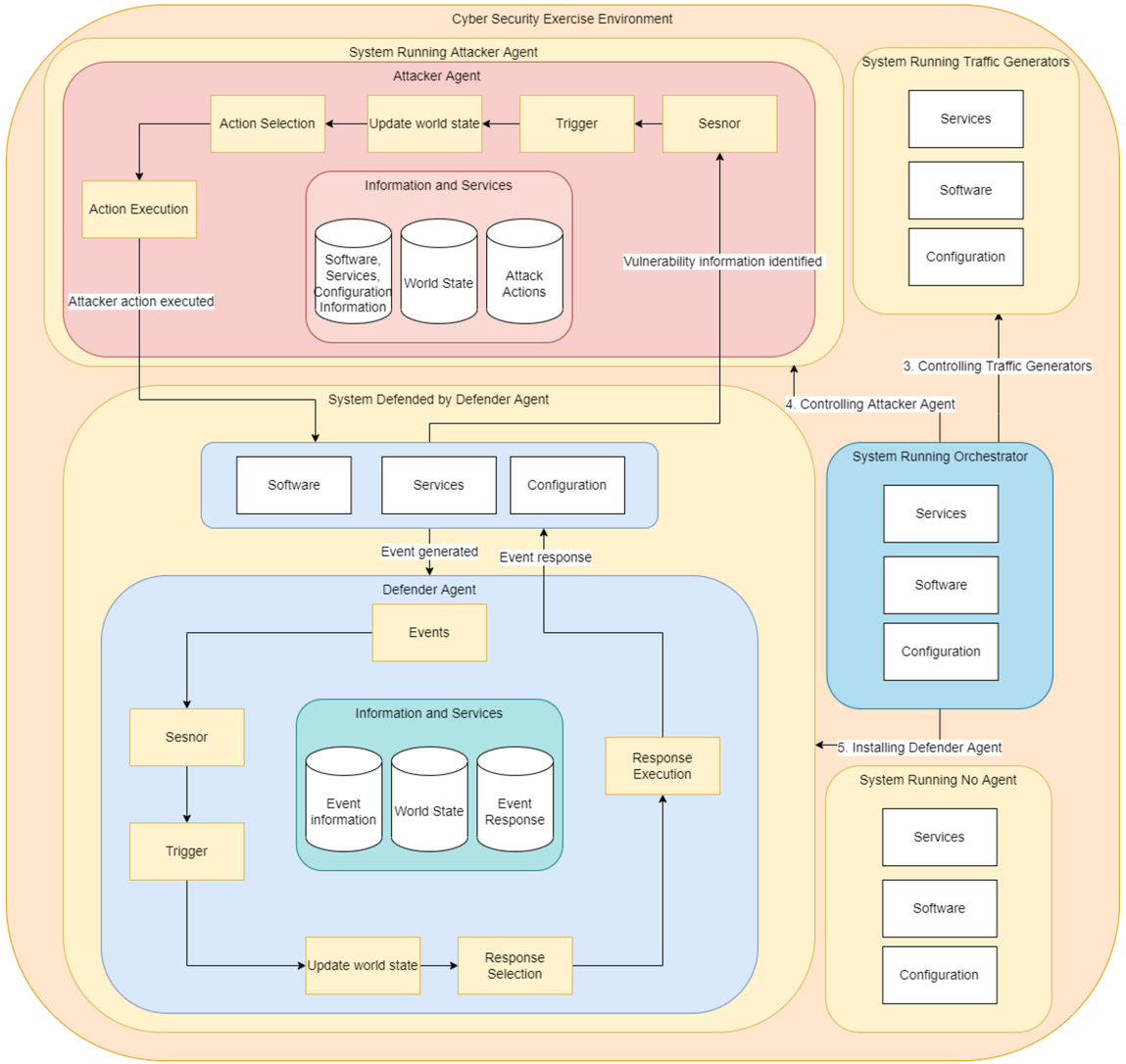
Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2022.102892 Get rights and content

Abstract

With the ever-changing cybersecurity landscape, the need for a continuous training for new cybersecurity skill sets is a requirement. Such continuous training programs can be delivered on platforms like cyber ranges. Cyber ranges support training by providing a simulated or emulated representation of a computer network infrastructure, besides additional training and testing services. Cyber attack and defense skills can be gained by attacking and defending a simulated or an emulated infrastructure. However, to provide a realistic training in such infrastructures, there is a need for necessary friction in the environment. Human teams, playing both attackers' and defenders' roles, provide this friction. Involving human teams in large-scale cybersecurity exercises is relatively inefficient and not feasible for standardizing training because different teams apply different tactics. Currently, the proposed solutions for cyber range training platforms focus on automating the deployment of the cybersecurity exercise infrastructure but not on the execution part. This leaves a room for improving exercise execution by adding realism and efficiency. This research presents an agent-based system that emulates cyber attack and defense actions during cybersecurity exercise execution; this helps provide realistic and efficient cybersecurity training. To specify agents' behavior and



Platform

Operational Cyber Security exercises Infrastructure

Computers & Security
Volume 122, November 2022, 102892

Use of cyber attack and defense agents in cyber ranges: A case study

Muhammad Mudassar Yamin, Basel Katt

Show more

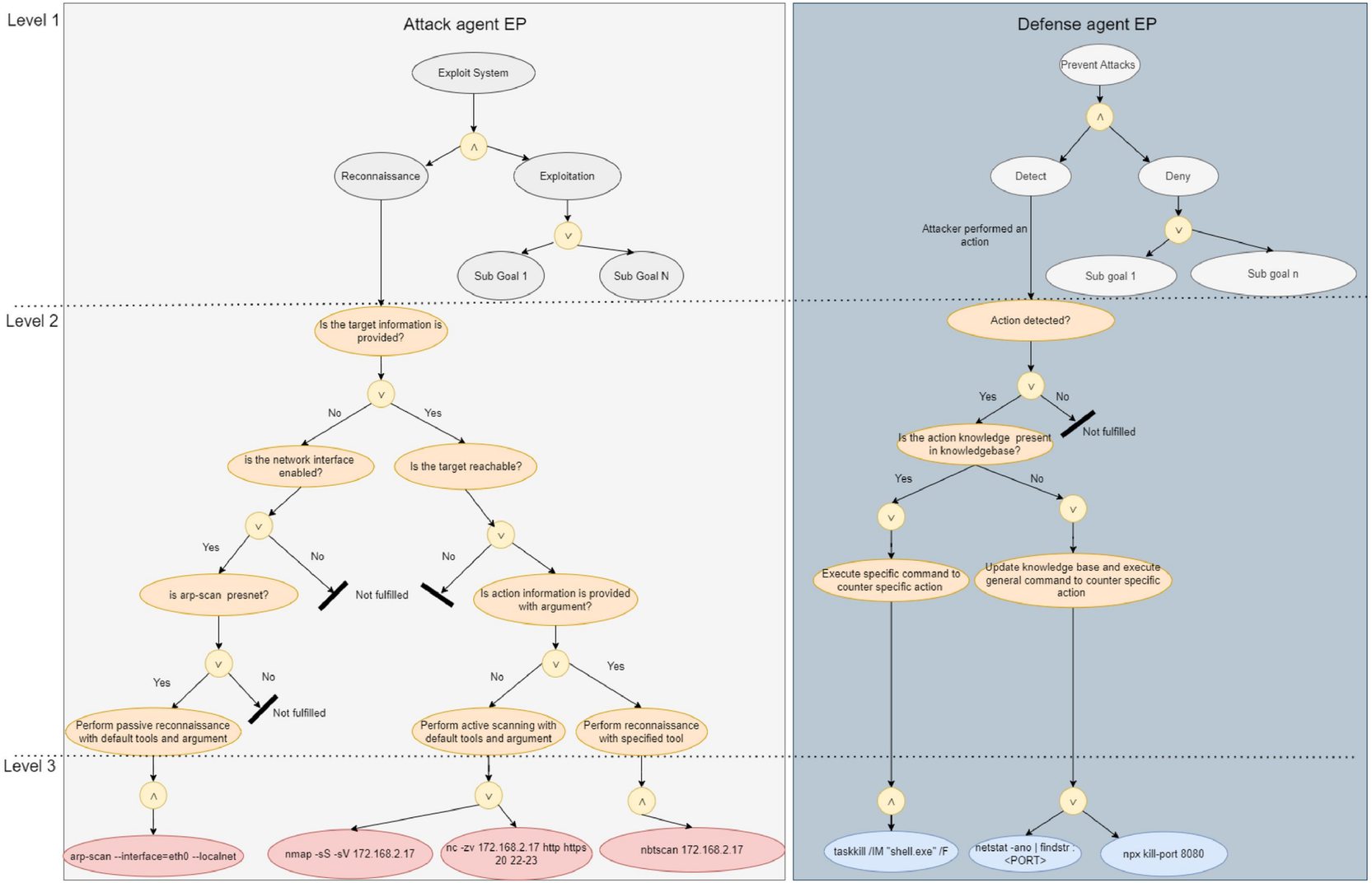
+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2022.102892

Get rights and content

Abstract

With the ever-changing cybersecurity landscape, the need for a continuous training for new cybersecurity skill sets is a requirement. Such continuous training programs can be delivered on platforms like cyber ranges. Cyber ranges support training by providing a simulated or emulated representation of a computer network infrastructure, besides additional training and testing services. Cyber attack and defense skills can be gained by attacking and defending a simulated or an emulated infrastructure. However, to provide a realistic training in such infrastructures, there is a need for necessary friction in the environment. Human teams, playing both attackers' and defenders' roles, provide this friction. Involving human teams in large-scale cybersecurity exercises is relatively inefficient and not feasible for standardizing training because different teams apply different tactics. Currently, the proposed solutions for cyber range training platforms focus on automating the deployment of the cybersecurity exercise infrastructure but not on the execution part. This leaves a room for improving exercise execution by adding realism and efficiency. This research presents an agent-based system that emulates cyber attack and defense actions during cybersecurity exercise execution; this helps provide realistic and efficient cybersecurity training. To specify agents' behavior and



Open Cyber Range

TRL7 Professional Artifact

Overview

What is OCR?

The Open Cyber Range (OCR) is project conducted by CR14, NTNU and TalTech and funded by Norway Grants and EAS. This project consists of cyber exercise platform hosted by the CR14 and a software development effort made create a new standard for describing and conducting cyber exercises. The following documentation covers the latter part. It covers functionalities of the developed tool-set, instructions on how to use them and guides for setting up similar toolchain.

The **Open Cyber Range software** consists of 3 main components:

- **SDL** - a.k.a. Scenario Definition Language allows to describe different aspects of a cyber exercise in a file format. Language designed by a research group inside NTNU is implemented into software by a language parser project. This parser is used in other components to integrate the SDL as the central part of the OCR software.
- **Deputy** - is a digital library for cyber exercise artifacts. While SDL allows to describe the exercise scenario in a single file, cyber exercises might be made up of thousands of large and repeatable artifacts. Deputy allows to store such artifacts and reuse them across the exercises. This reduces the load for storage resources and more importantly allows easy reusability to save exercise administrator time and money.
- **Ranger** - is a management application that serves a single gateway for the users of the OCR software. It offers three roles for users: exercise participant, exercise manager and exercise client. It takes of full the business process cycle. From the initial exercise request to deploying it into the virtualized environment up to recognizing learning objectives with the exercise participants.

SDL > Example Script

SDL Example Script

An example script of a full exercise containing all SDL building blocks.

```
name: example-sdl
stories:
  story-1:
    speed: 1
    description: "This is a story for the general user in the scenario"
    scripts:
      - script-1
  story-2:
    speed: 1
    description: "This is a story for the developer in the scenario"
    scripts:
      - script-2
  story-3:
    speed: 1
    description: "This is a story for the red team in the scenario"
    scripts:
      - script-3

scripts:
    #General user
    script-1:
        description: "Imitates the daily activities of general use"
        start-time: 0
        end-time: 10 hour
        speed: 1
```

https://documentation.opencyberrange.ee/

Open Cyber Range

Most Important Technical Collaboration Project Between Norway and Estonia

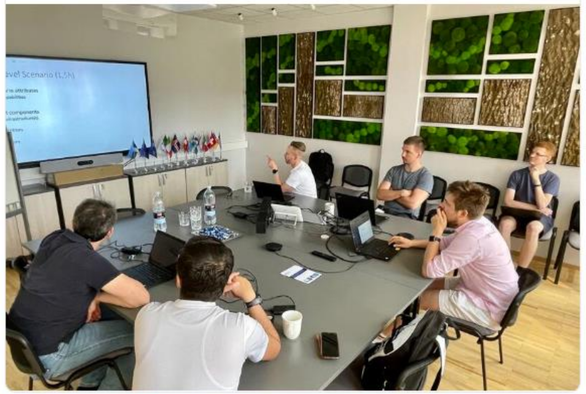
CR14
2,040 followers
1yr • Edited •
+ Follow

This week, we welcome Open Cyber Range (#OCR) partners in #CR14: Kaitseministeerium / Ministry of Defence of Estonia, TalTech – Tallinn University of Technology and the Norwegian University of Science and Technology (NTNU). "During this get-together, we aim to create a standard in order to share exercises-as-code between Cyber Ranges," highlighted Kaarel Allemann, Software Development Lead for OCR, one of the goals. "A lot can be done online, but nothing beats a face-to-face meeting every now and then", he added.

OCR project aims to develop cyber security thinking in private companies and the education sector. Within 3 years, our team will:
📍create a platform for (new) cybersecurity companies to develop, test and validate their innovative products,
📍create a launch pad for new products to emerge into the market,
📍promote security thinking in the private sector and
📍support cyber security education activities.

⏰ Stay tuned for future updates and be ready to test your new products already in late autumn!

#GreenICTprogramme #NCR #opencyberrange #cyberrange #cybersecurity



Norwegian Embassy in Tallinn
24 November 2023 ·

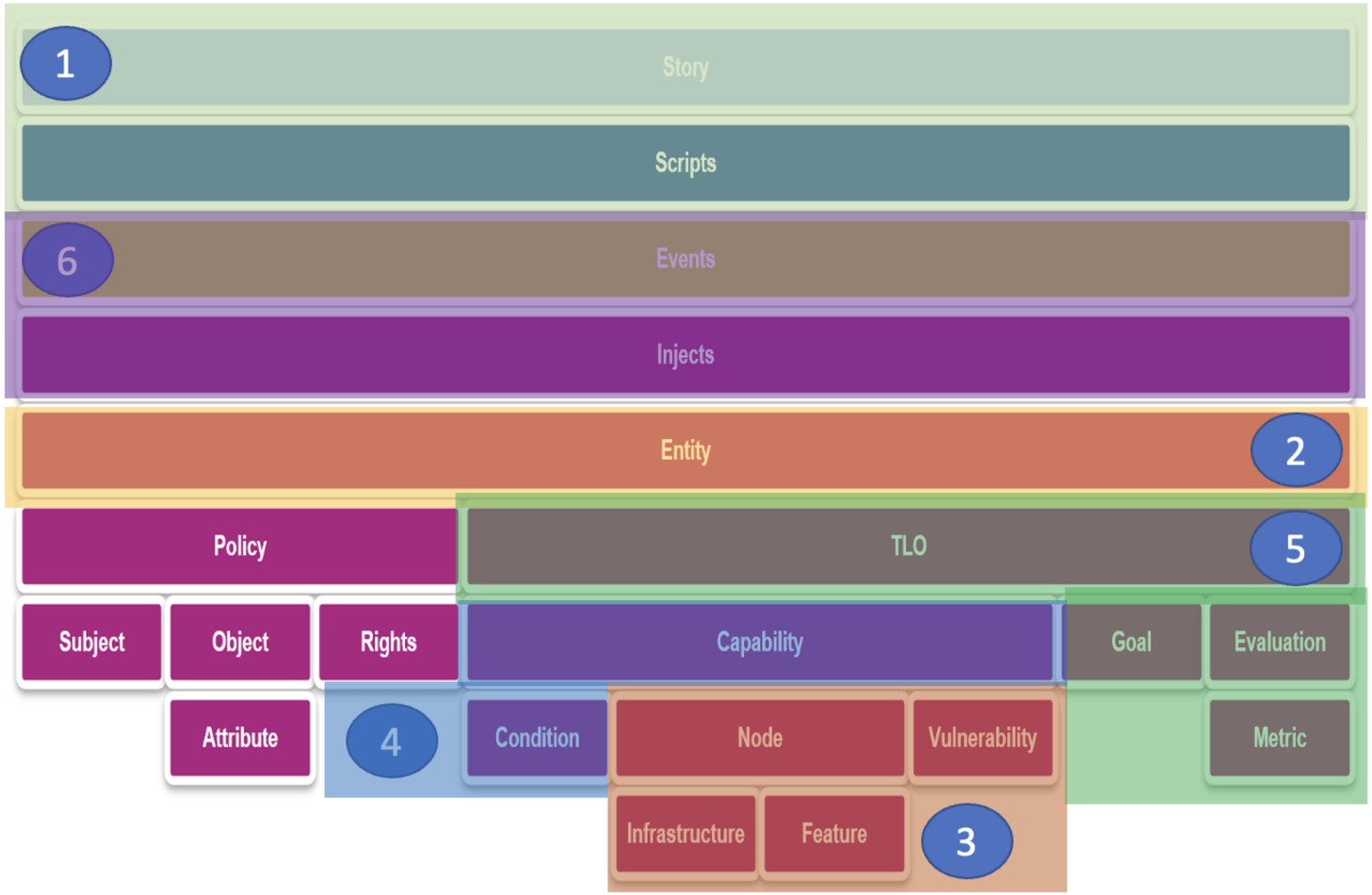
Kuna nii Norra kui ka Eesti on mõlemad väga digitaliseeritud ühiskonnad ning küberturvalisus on mõlema riigi jaoks oluline, siis oli CR14 külastus loogiline osa programmist. Cyber Range #CR14 kutsutakse küberharjutusväljade multiversumiks. CR14 on Kaitseministeeriumi asutatud sihtasutus, kus saab oma küberteadmisi testida ja õppuseid korraldada. Oleme uhked, et ka Norra toetusega ja koostöös Norra teadus- ja tehnikaülikooliga NTNU on arendatud avatud küberharjutusväli Open Cy... **See more**

See translation

Scenario Definition Language

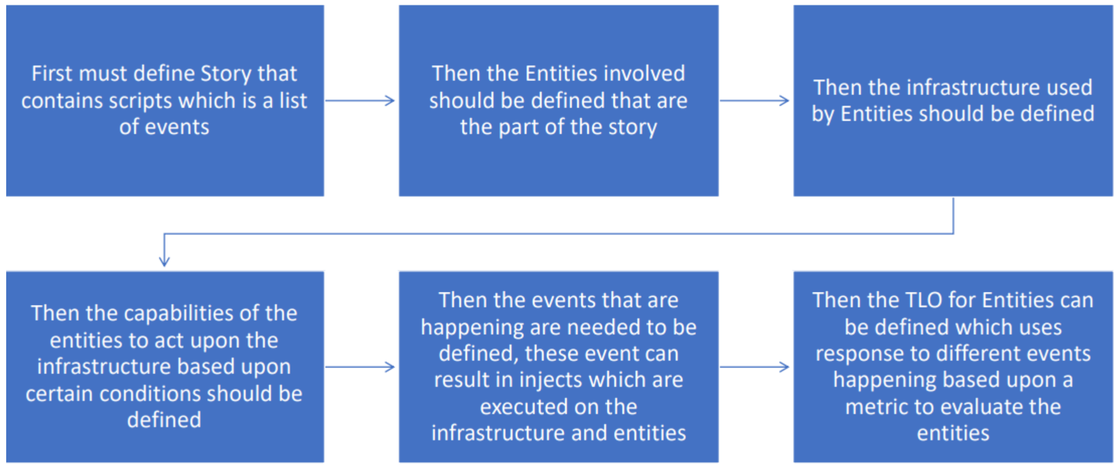
SDL Components

- Story
  - Scripts/Sub story
- Entity/Agents/Character
- Infrastructure/World
- Conditions/Objects
- Events/Events
  - Injects
- TLOs
  - Goal
  - Capability
  - Evaluation



Cyber Security Exercises

Scenario Generation Using Mult Agent LLMs



Cyber Security Exercise Preparation Process

Exercise Design Framework with LLMs

Yamin, M. M., Hashmi, E., Ullah, M., & Katt, B. (2024). Applications of LLMs for Generating Cyber Security Exercise Scenarios.

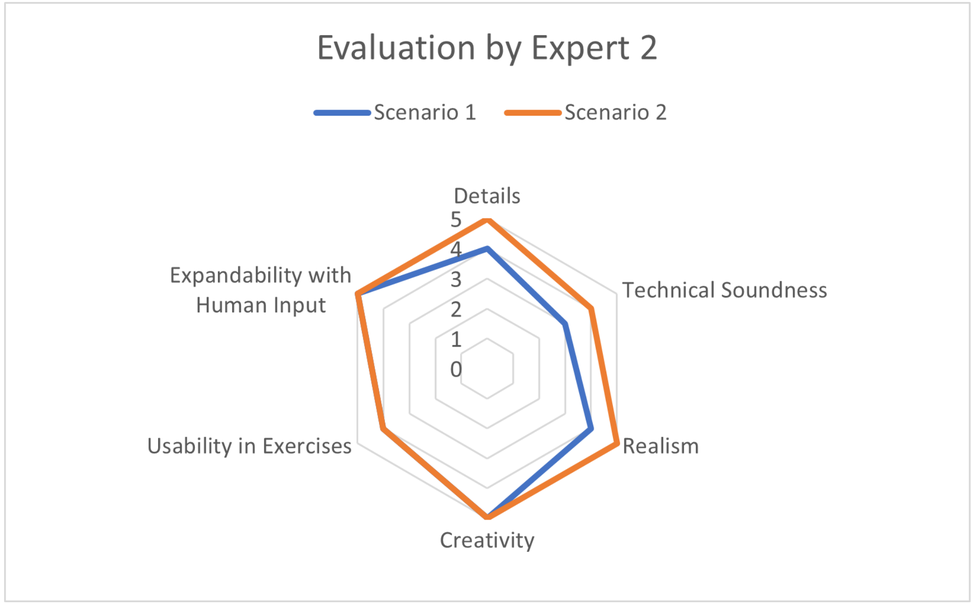
Cyber Security Exercises

**Main Scenario: **

Your organization, a mid-sized company in the finance industry, has been targeted by an advanced persistent threat (APT) group. The APT group has been able to gain unauthorized access to your network and has been actively manipulating and exfiltrating sensitive data for several months.

As the incident response team, you have been alerted to the situation and are tasked with containing the attack, identifying the scope of the breach, and mitigating any further damage. Your team consists of security experts from various departments within the organization, including IT, legal, and compliance.

Generated Scenario Sample



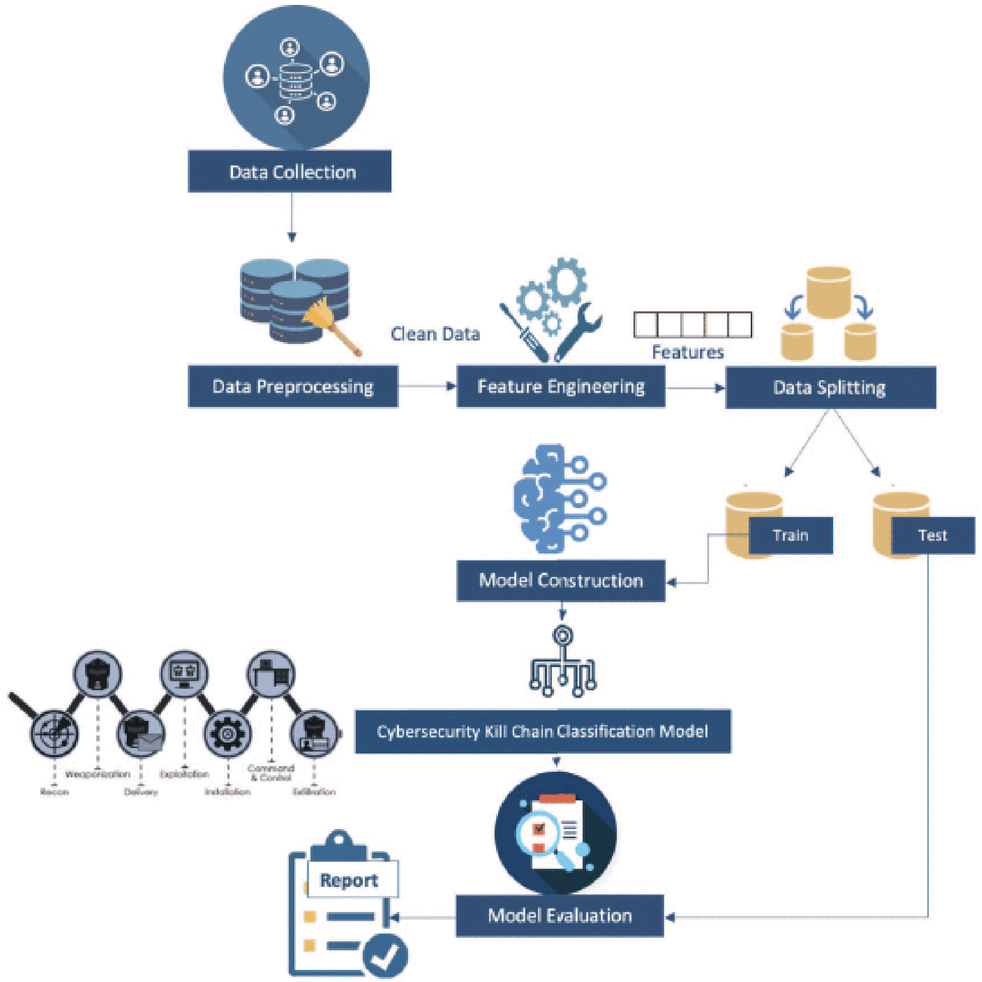
Scenario Evaluation

Yamin, M. M., Hashmi, E., Ullah, M., & Katt, B. (2024). Applications of LLMs for Generating Cyber Security Exercise Scenarios.

Skill Assessment for Cybersecurity Exercises

Reconnaissance	• Identification, selection and profiling of target
Weaponization	• Coupling of remote access torjan with an exploit
Delivery	• Transmission of cyber weapon to targeted environment
Exploitation	• Trigerring the attacker's payload on target system
Installation	• Installation of back door and maintaining persistence
Command & control	• Outbound internet controller servers to communicate
Action on objectives	• Data exfiltration, network spreading, system disruption

Seven Phases of the Cyber kill Chain



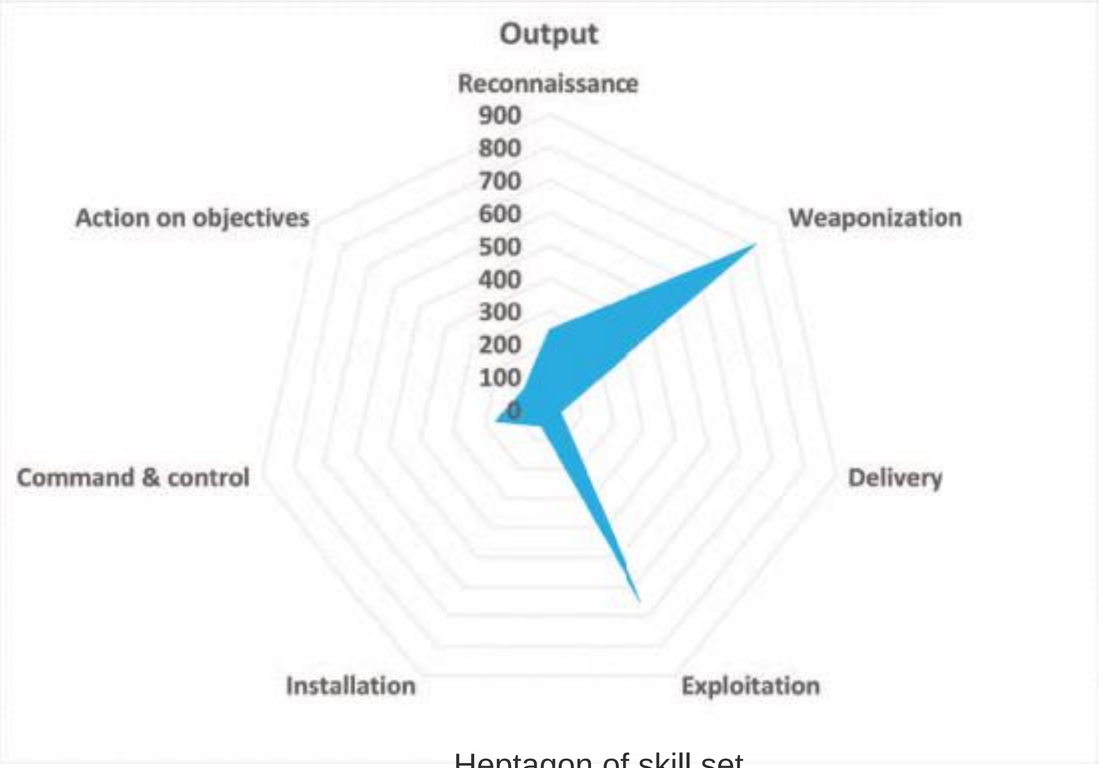
Proposed Methodology for Cybersecurity Kill Chain Classification

https://ieeexplore.ieee.org/abstract/document/10410697

Skill Assessment for Cybersecurity Exercises

Method	Precision	Recall	F-Measure
LR [30]	0.97	0.91	0.94
MNB [31]	0.94	0.76	0.82
RF [33]	0.97	0.95	0.96
SVM [32]	0.97	0.94	0.95
Ensemble [34]	0.98	0.94	0.96
Proposed	**0.98**	**0.98**	**0.98**

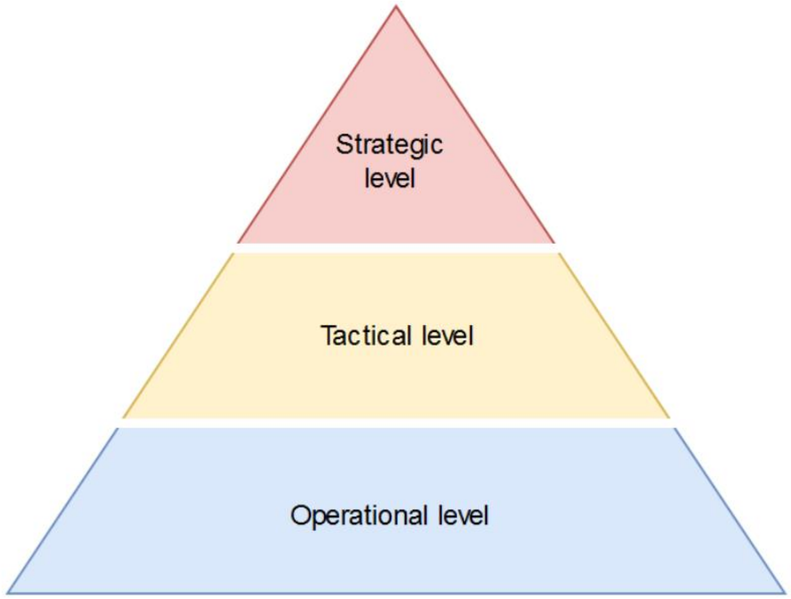
Card Model Comparison with Traditional Machine Learning Models



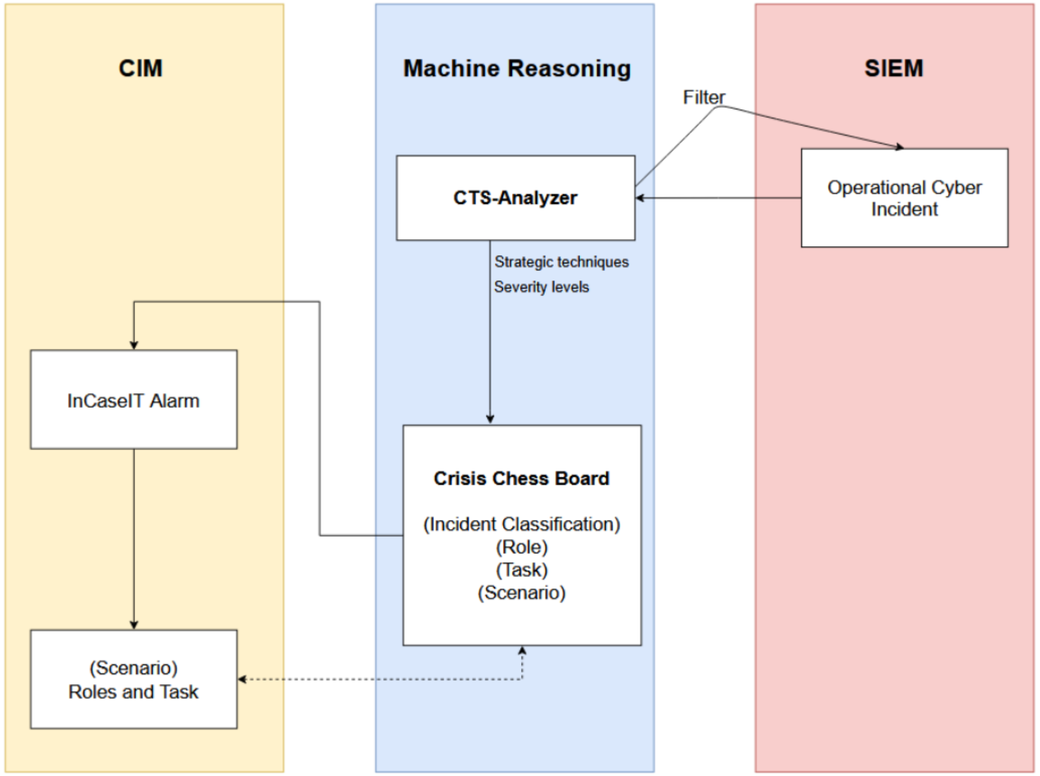
Heptagon of skill set

https://ieeexplore.ieee.org/abstract/document/10410697

AI-Driven Cyber Security Analysis

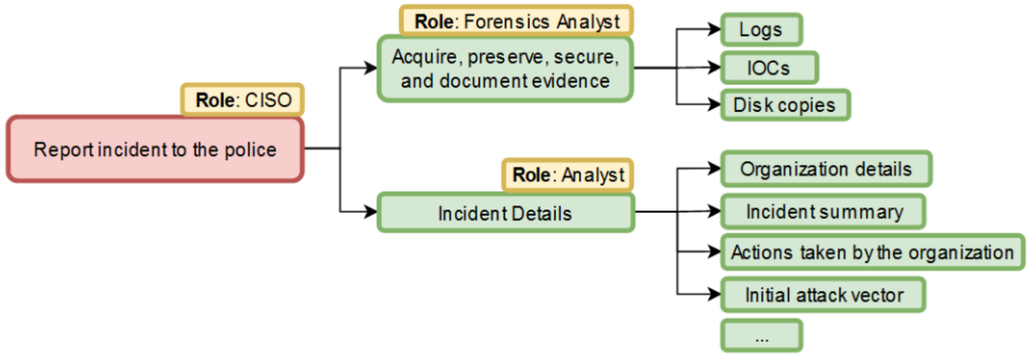


NIST Framework Tiers



Information flow between CIM, CCB, and SIEM systems

AI-Driven Cyber Security Analysis



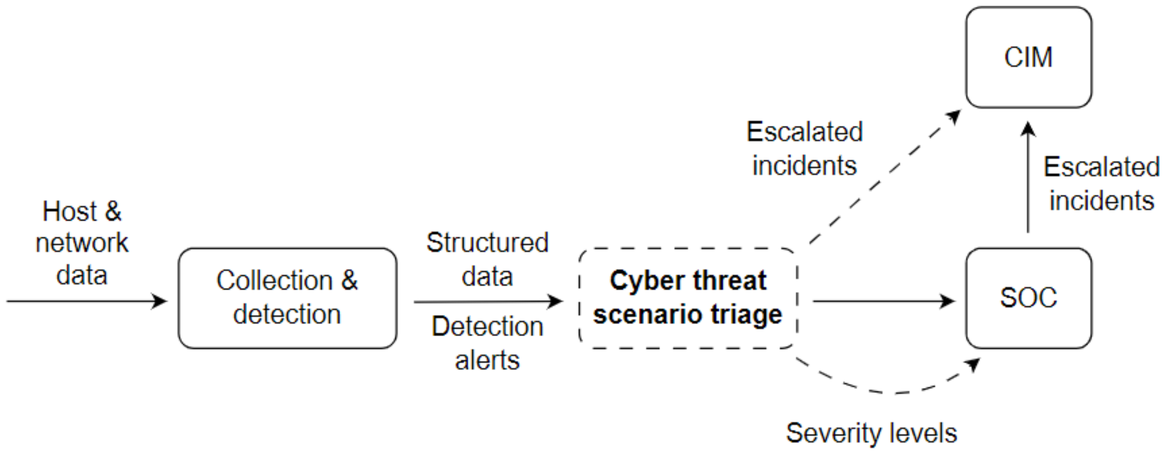
Mapping of Strategic to Operational tasks

OPENING

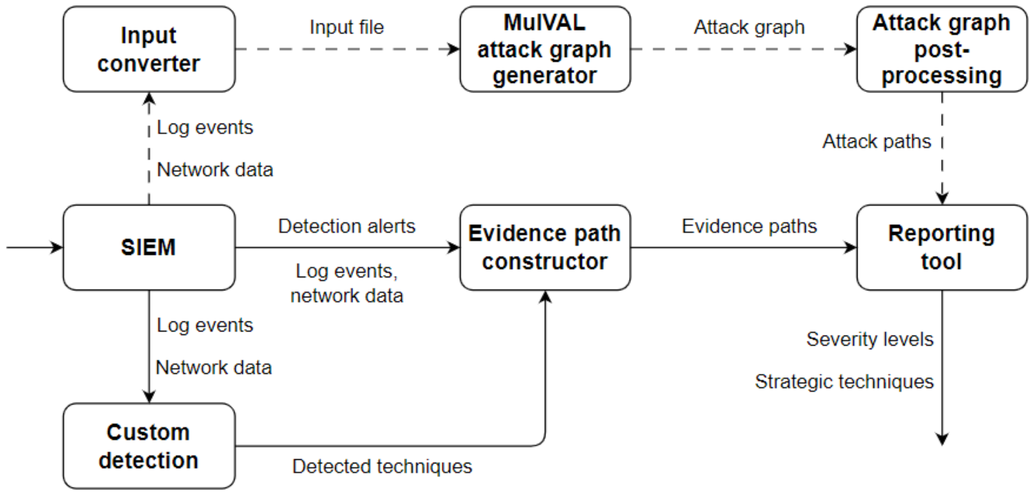
Task	*Role*	*Description*	*Priority*	*Done*
Schedule Initial Status Meeting and alert personnel	Crisis Manager	Organize an immediate meeting with all key stakeholders, including upper management and relevant department heads, to discuss the current situation, share initial findings, and outline next steps.	1	
Determine scope of the ransomware attack	CISO	Determine the scope of the attack by identifying all impacted systems, services, and data. Information will be used to understand the extent of the damage and prioritizing recovery efforts.	1	
Identify attack vector	IT Security Team Lead	Identify initial attack vector used by the attackers to get access to the organization's systems.	1	
Preserve evidence and initiate a forensic investigation	CISO	Secure and preserve all relevant digital evidence, including logs and infected systems, to facilitate a thorough forensic investigation.	1	
Assess financial impact and risk exposure	CFO	Estimate the financial implications of the ransomware attack, considering factors such as potential loss of revenue, remediation costs, and regulatory fines.	2	
Create a priority list for recovering systems	CTO	Develop a list of critical systems and services that need to be restored first, considering business needs, customer impact, and regulatory requirements. This list will be important in the restoration process.	3	
Develop a communication strategy for stakeholders	Communication Manager	Prepare a plan for communicating with internal and external stakeholders, including employees, customers, and partners, about the incident and the organization's response. The plan should help restore the reputation of the organization.	2	
Isolate the Infected Systems	CISO	Isolate the infected system(s) from the network and the internet to prevent the spread of the ransomware to other systems.	1	

Crisis Chess Board Incident Plan

Cyber Threat Scenario Analyzer

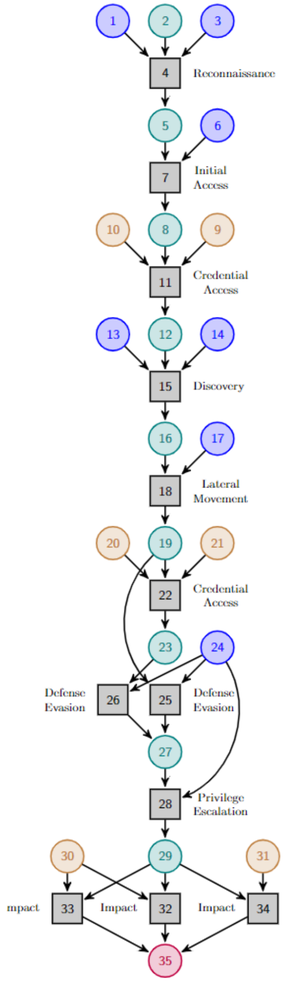


The triage assigns severity levels and automatically escalates incidents that would be otherwise escalated by SOC analysts manually



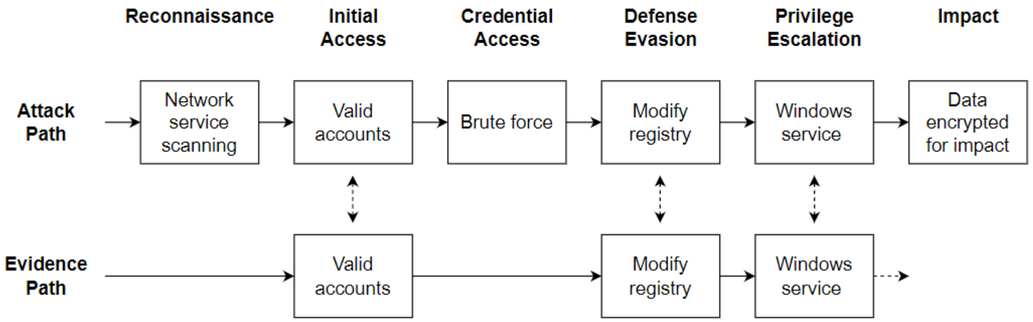
Design of the prototype implementation of the CTS Analyzer.

Cyber Threat Scenario Analyzer



ID	Value
1	networkService(*10_11_2_113*, _, *tcp*, _, _).
2	accessAllowed(*10_255_11_28*, *10_11_2_113*, *tcp*, _).
3	externalActor(*10_255_11_28*).
4	T1595 – Active Scanning
5	networkConnection(*2*, *authentication*, *10_11_2_113*, *tcp*, _).
6	hasAccount(_, *user*, *10_11_2_113*, *windows*).
7	T1078 - Valid Accounts
8	account(*2*, *authentication*, *user*, _, *10_11_2_113*, *windows*).
9	multifactorAuthentication(*no*).
10	strongPasswordPolicy(*no*).
11	T1110 – Brute Force
12	account(*2*, *authentication*, *root*, _, *10_11_2_113*, *windows*).
13	networkService(*10_11_1_10*, _, *tcp*, _, _).
14	accessAllowed(*10_11_2_113*, *10_11_1_10*, *tcp*, _).
15	T1046 – Network Service Discovery
16	networkConnection(*2*, *authentication*, *10_11_1_10*, *tcp*, _).
17	hasAccount(_, *user*, *10_11_1_10*, *windows*).
18	T1021 – Remote Services
19	account(*2*, *authentication*, *user*, _, *10_11_1_10*, *windows*).
20	multifactorAuthentication(*no*).
21	strongPasswordPolicy(*no*).
22	T1110 – Brute Force
23	account(*2*, *authentication*, *root*, _, *10_11_1_10*, *windows*).
24	installed(*10_11_1_10*, *windows*).
25	T1112 - Modify Registry
26	T1112 - Modify Registry
27	file(*2*, *integrity*, *10_11_1_10*, *registry*).
28	T1543.003 – Windows Service
29	system(*2*, *authorization*, *10_11_1_10*, *root*).
30	dataBackup(*10_11_1_10*, *no*).
31	encryptedDisk(*10_11_1_10*, *no*).
32	T1486 – Data Encrypted for Impact
33	T1485 – Data Destruction
34	T1565.001 – Data Manipulation – Stored Data Manipulation
35	file(*2*, *integrity*, *10_11_1_10*, _).

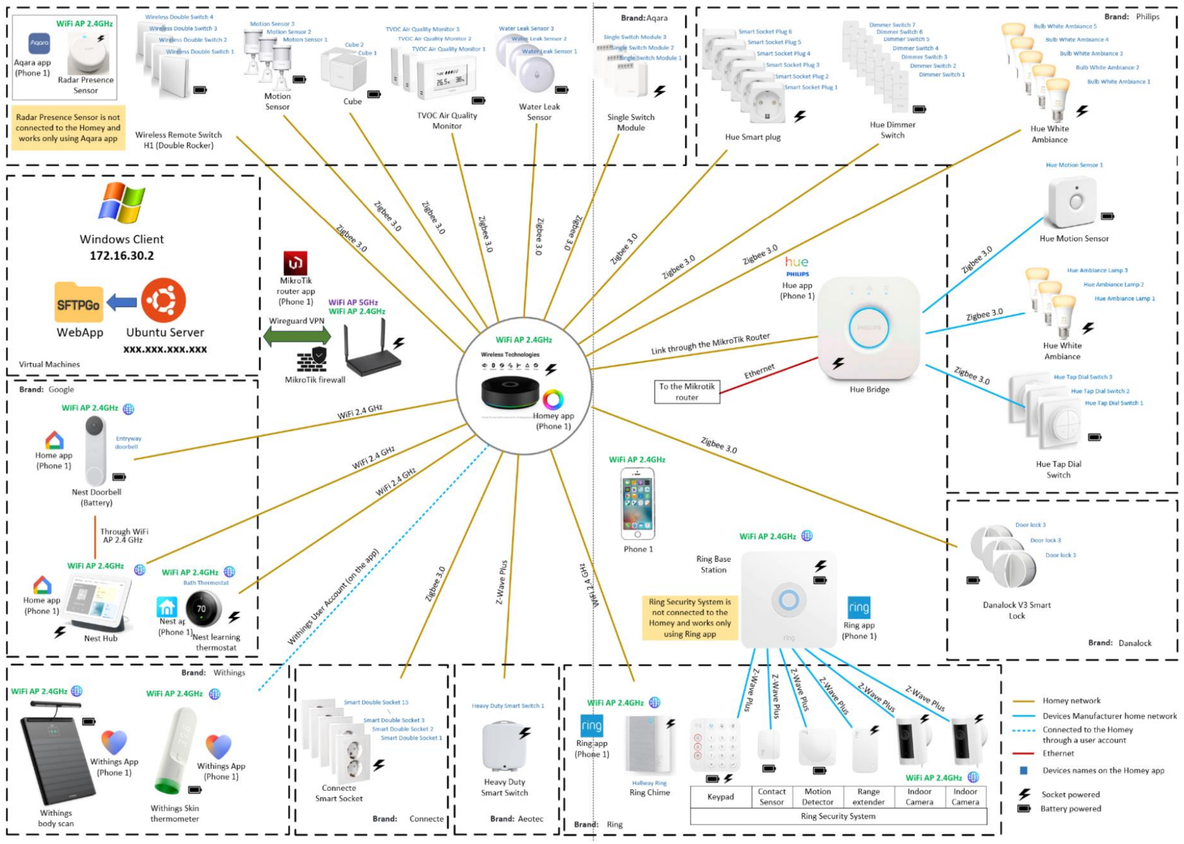
Attack graph generated based on host and network data



Path matching of attack path and evidence path. Names of kill chain phases are above the paths

Hybrid Cyber Security Exercise Scenarios

Smart Home Hybrid Testbed



Front view

Side view

Some Sample Exercises

Full Scale Exercises

Fullskala krisehåndteringsøvelse i Norwegian Cyber Range

Foto: Kenneth Nordahl-Pedersen

Av Guro Wang Øverli, seniorrådgiver, kommunikasjonsavdelingen, Norges teknisk-naturvitenskapelige universitet

Publisert: 12.11.21 16:08 **Del**

Artikkelen er over 2 år gammel

INNSENDT Norwegian Cyber Range avholdt nylig den første fullskala

https://www.oa.no/fullskala-krisehandteringsovelse-i-norwegian-cyber-range/s/5-35-1433118

Sikt – Norwegian Agency for Shared Services in ... + Follow

2,529 followers

1yr • Edited •

Øvelse Morris er gjennomført, og kunnskapssektoren har fått øvd på å beskytte informasjonsverdiene i norsk forskning og utdanning

I dag har Cybersikkerhetssenter for forskning og utdanning i Sikt, i samarbeid med Norwegian Cyber Range (NCR) ved NTNU, holdt den aller første felles cybersikkerhetsøvelsen for kunnskapssektoren

– Vi vet at forskning og utvikling er særdeles utsatt for hendelser og forsøk på angrep i cyberdomenet i disse dager. Nettopp derfor er det svært gledelig at hele 17 virksomheter har gått sammen om å øve sammen i et reelt og tidsaktuelt scenario, sier produktområdeleder for Cybersikkerhetssenteret i Sikt, Bjørn Helge Kopperud.

Øvelsen har foregått i en virtuell verden. Denne verdenen har mye av det samme som du finner i den virkelige verden – aviser, sosiale medier, e-post og logger, men også cybertrusler som ligger i det skjulte og lurer

– Det har vært inspirerende å se engasjementet og pågangsmotet til deltakerne, og jeg er sikker på at vi er litt bedre rustet til å håndtere hendelser nå enn vi var i dag tidlig, avslutter Bjørn

Det finnes ufattelig mye verdifull kunnskap og informasjon i Norsk kunnskapssektor. I dag har vi øvd for å være bedre rustet til å beskytte disse verdiene i fremtiden.

Tusen takk til alle som har deltatt og til alle som har gjort denne øvelsen mulig!

#cybersikkerhet #cybersecurity

See translation

Contact Us My side Change language Search

Full-scale exercise of a cyber attack

Last week, Gjøvik municipality carried out a full-scale exercise where the theme was cyber attacks.

It is the first time in Norway that such a large exercise with this theme has been carried out. Gjøvik was first out, in the next few weeks both Land municipalities and Vestre Toten municipality will be in the fire.

https://www.gjovik.kommune.no/aktuelt/fullskala-ovelse-pa-et-cyberangrep.51203.aspx

Norwegian Cyber Range

Virtual Tour

Questions?

Muhammad.m.yamin@ntnu.no