This article has been published in:
M. Leitner et al., "AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research," in Proceedings of the European Interdisciplinary Cybersecurity Conference, New York, NY, USA, Nov. 2020, pp. 1–6, https://doi.org/10.1145/3424954.3424959

AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research

Maria Leitner
AIT Austrian Institute of Technology
Vienna, Austria
maria.leitner@ait.ac.at

Maximilian Frank
AIT Austrian Institute of Technology
Vienna, Austria
maximilian.frank@ait.ac.at

Wolfgang Hotwagner
AIT Austrian Institute of Technology
Vienna, Austria
wolfgang.hotwagner@ait.ac.at

Gregor Langner
AIT Austrian Institute of Technology
Vienna, Austria
gregor.langner@ait.ac.at

Oliver Maurhart
AIT Austrian Institute of Technology
Vienna, Austria
oliver.maurhart@ait.ac.at

Timea Pahi
AIT Austrian Institute of Technology
Vienna, Austria
timea.pahi@ait.ac.at

Lenhard Reuter
AIT Austrian Institute of Technology
Vienna, Austria
lenhard.reuter.fl@ait.ac.at

Florian Skopik
AIT Austrian Institute of Technology
Vienna, Austria
florian.skopik@ait.ac.at

Paul Smith
AIT Austrian Institute of Technology
Vienna, Austria
paul.smith@ait.ac.at

Manuel Warum
AIT Austrian Institute of Technology
Vienna, Austria
manuel.warum@ait.ac.at

ABSTRACT

With the evolution of threats and attacks and the speed of automation, new modern training and learning environments are needed to support the challenges of digital organizations and societies. In recent years, cyber ranges, i.e., virtual environments that support the simulation of diverse infrastructures, have emerged and are often utilized for cyber security exercises or training. With these environments, organizations or individuals can increase their preparedness and dexterity, for example, by training to identify and mitigate incidents and attacks. In this paper, we present the AIT Cyber Range which was designed based on several principles such as scalability, flexibility and the utilization of Open Source technologies. This paper outlines the building blocks of the architecture and implementation: computing platform, infrastructure provisioning, software provisioning and scenario engine. Furthermore, the implementation is demonstrated by three use cases: cyber exercises, training as well as security research and development. For future work, we aim to further extend the building blocks and to address federation and interoperability with other cyber ranges.

CCS CONCEPTS

• **Security and privacy** → *Security services*; • **Computer systems organization** → *Real-time systems*;

EICC 2020, November 18, 2020, Rennes, France

ACM ISBN 978-1-4503-7599-3/20/11.
https://doi.org/10.1145/3424954.3424959

KEYWORDS

cyber range, information security, testbed, cyber exercises, training

ACM Reference Format:
Maria Leitner, Maximilian Frank, Wolfgang Hotwagner, Gregor Langner, Oliver Maurhart, Timea Pahi, Lenhard Reuter, Florian Skopik, Paul Smith, and Manuel Warum. 2020. AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research. In *European Interdisciplinary Cybersecurity Conference (EICC 2020), November 18, 2020, Rennes, France.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3424954.3424959

1 INTRODUCTION

Information security has become an integral part of our society. Threats and attacks evolve constantly and the response and mitigation can become challenging for organizations and individuals. With increasing system automation and digitalization, however, it becomes even more important that learning and training methods for information security need to evolve too. In particular, a highly realistic (i.e. dynamic and interconnected) training environment would be preferred. For information security, learning environments, training and competitions have been developed in the past 15 years. For example, many cyber security exercises and training courses have been developed to increase capabilities, skills and competences of individuals and strengthen the resilience and preparedness of organizations against threats and attacks.

Often, these cyber exercises are conducted on top of virtual environments, often called *Cyber Ranges* or *cyber security testbeds* that simulate ICT infrastructures of, for example, small-, medium or large organizations (public or private). Literature often refers to cyber ranges as virtual environments using virtualization software but others may include also physical components (see, e.g., [3, 5, 14, 21]). So far, different approaches use the term "cyber range",

for example, such as a university lab or a classified security environment [21]. Hence, architectural and implementation details matter for analysis and comparison.

Cyber ranges support experiential learning by for example hosting training (e.g., [8, 12, 15]) or cyber exercises (e.g., [7, 19]). An advantage is that cyber ranges provide a safe environment for trainees. Production systems are normally unaffected by training or exercises. All actions are happening within the cyber range testbed.

In this paper, we outline the architecture, implementation and use cases of the AIT Cyber Range. The AIT Cyber Range's aim is to provide a flexible and scalable architecture that consists of four building blocks: computing platform, infrastructure provisioning, software provisioning and scenario engine. As our development is primarily focused on Open Source technology, these building blocks were implemented using several technologies, e.g., OpenStack and TerraForm providing flexibility and scalability. Both technologies allow for the rapid and modular deployment of infrastructure and software services. To demonstrate our system, we describe three use cases on the infrastructure: cyber exercises, training as well as security research and development. Each use case outlines the versatility of the cyber range. Overall, the use cases contribute to building competencies and skills but also to investigate and contribute to new research directions (e.g., simulation and detection of attacks).

The rest of the paper is structured as follows. Section 1 introduces and motivates the challenges. Section 2 outlines related work within the context of cyber ranges and cyber security testbeds. Section 3 describes the requirements and architectural decisions. Section 4 outlines the implementation. Section 5 demonstrates the cyber range using three use cases. Lastly, Section 6 concludes the paper.

2 BACKGROUND

Cyber ranges and cyber security testbeds. In a survey by [3], several cyber ranges are reviewed and the term "cyber range" is investigated. Furthermore, the NIST [14] defines that "*cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment*". The European Cyber Security Organisation (ECSO) [5] defines cyber ranges as "*a platform for the development, delivery and use of interactive simulation environments. A simulation 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. [...].*" Furthermore, authors in [21] systematically assess cyber ranges and, for example, the technology used. It provides an extensive overview of cyber ranges (e.g., utilized technology and tools). Design considerations when hosting such cyber security testbeds have to be taken into account (e.g.,[2, 8]).

As the survey in [21] shows, there are a vast number of testbeds or cyber ranges. It is challenging to compare our development to other cyber ranges without more details. First of all, not every testbed or cyber range has publicly available information on architecture or implementation. Also identifying potential testbeds and cyber ranges might be cumbersome. As a starting point to compare architectural building blocks, the functional architecture of cyber ranges given in [21] could be utilized. For example, most of the building blocks are also represented in the AIT cyber range. Furthermore, we use a very similar vocabulary as outlined in the taxonomy suggested by [21] in the AIT Cyber Range specification. For example, we use the same terminology for "Scenarios", "Storylines". However, "Environment" is an infrastructure in our design specification. These considerations support that functional aspects or designs could be compared to other cyber ranges. In particular, the details are essential. A comparative analysis, for example, might need more in-depth exchange between cyber range providers. This publication aims to share architectural designs and implementation specifications in order to start exactly this conversation and foster the exchange of results.

Cyber exerises. A variety of cyber exercises has emerged in the past 15 years. Cyber security exercises may aim at different goals (e.g., to build competences, to assess competences or to just have fun). Cyber security exercises can be structured and designed in various ways (cmp. [6]). For example, Capture-The-Flag exercises (e.g., iCTF [18], DEFCON CTF, NYU-CSAW) are designed so that participants (teams or individuals) capture a certain flag (e.g., a file or text). CTFs often use specifically designed platforms [11]. Other examples are cyber security exercises or cyber defense exercises (CDX) (e.g., [10, 19]) that are often hosted in virtual environments such as cyber ranges. Lastly, table-top exercises are also a common method to conduct cyber exercises with participants from various domains (cmp. [4, 9]). They often use cards, board games or apps to support their game.

3 AIT CYBER RANGE: MOTIVATION AND ARCHITECTURE

3.1 Motivation

The motivation to start and develop our own infrastructure and software provisioning was driven by several aspects that we wanted to address and at the time, about 5 years ago, there was no open source infrastructure or software available. The motivation to develop a cyber range was: (1) to develop individual threat scenarios that can be hosted and executed in a planned way; (2) to establish industrial control systems (ICS) on the cyber range; (3) to enable a flexible simulation infrastructure that could be customized for different occasions and customers; (4) to enable scalability from small to large scenarios and infrastructures; and (5) to utilize open source technology and to contribute to this community. Based on these requirements, we developed an architecture (see Section 3.2) and implementation (see Section 4).

3.2 Architecture

This section describes the AIT Cyber Range architecture and its components solely from a conceptual point of view without addressing implementation details which are be discussed in Section 4.

The AIT Cyber Range architecture consists of four system modules (i.e. building blocks) which are shown in Figure 1. These modules in combination are able to fulfil the above mentioned requirements. Modules all have a distinct purpose and are only loosely

dependent on each other, so as to make changing the underlying technologies or implementation as easy as possible.

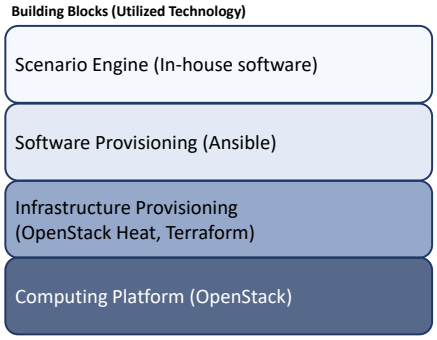

Figure 1: AIT Cyber Range: Modules and utilized Technology

3.2.1 Computing Platform. At the core of every cyber range is the ability to simulate and integrate systems to build complex networked infrastructure setups. The computing platform is the module that facilitates and makes this possible. This role can be fulfilled by most modern Infrastructure as a Service platforms (e.g., OpenStack, AWS) or virtualization stacks (e.g., VMware). Selecting which computing platform to use is very important as it will directly influence what can be simulated and integrated into the cyber range.

3.2.2 Infrastructure Provisioning. Cyber security testbeds are one of the core features of a cyber range. The infrastructure provisioning module is the component that is used to create these testbed configurations and orchestrate them on the computing platform. For this a software solution is needed with which it is possible to efficiently design, create, store and orchestrate complex infrastructure networks.

Many of the technologies that can be used as computing platforms already have capabilities which can be used to implement this module integrated in their feature set (e.g., OpenStack Heat Templates), but there also exist solutions which provide the required features for multiple different computing platform technologies (e.g., Pulumi or Terraform). Supporting multiple computing platforms on the infrastructure provisioning level has the advantage of being more flexible when choosing a computing platform.

3.2.3 Software Provisioning. Using the computing platform and infrastructure provisioning modules it is possible to create large complex networked infrastructure. The software provisioning module is used to add actual functionality to machines in these cyber security testbeds. This means while the computing platform and infrastructure provisioning is used to model and create the connections and system parameters (e.g., CPU count) for a testbed, the software provisioning module is used to model the roles the machines have within the scenario.

This makes the software provisioning module an essential application deployment and configuration management tool for use within the cyber range. Therefore, it can be realized with one of the many already available software solutions for this use case (e.g., Ansible, Puppet).

3.2.4 Scenario Engine. The scenario engine is the module that is used to define the flow of a cyber range scenario. It turns the static infrastructure created by the other three modules into a living system. This module is mainly used to extend the functionality of the AIT Cyber Range to support not only static use cases, such as security test beds, but also dynamic cyber range activities, such as cyber exercises.

The scenario engine must support two basic features to achieve this. First, it needs to be possible to define a series of injects (i.e., actions within the context of a scenario, e.g., sending of a message) during development of a scenario. Second, during the execution of a cyber exercise these injects need to be automatically executed to establish the dynamic scenario to which cyber exercise participants react.

Depending on the level of sophistication of the scenario engine, it might be possible to employ it in other cyber range use cases such as security research. A scenario engine that supports the definition of complex cyber attacks as injects can be used to automate an attack chain. Such automation can, for example, be useful for security research where repeatability is important for the verification of research results.

4 AIT CYBER RANGE: IMPLEMENTATION

This section gives a brief description of the technological design decisions and implementation of the AIT Cyber Range.

4.1 Computing Platform

As already mentioned in Section 3.2.1, there are many suitable software solutions available that can fulfil the function of a computing platform. Alternatively, it would also be possible to develop such a platform specifically for usage in a cyber range, if the resources for this are available. The AIT Cyber Range uses a self hosted OpenStack cluster as its compute engine. OpenStack was chosen as our computing platform due to its open source nature and high level of adoption.

The AIT Cyber Range consists of a mostly default OpenStack (https://www.openstack.org/) configuration run on multiple Ubuntu-based nodes. Within our research group we have multiple teams that require access to the cyber range for use in various research topics. Testbeds of these teams needed to be isolated from each other. For this we utilized OpenStacks tenant isolation features. Each team is setup within their own OpenStack domain that is only able to access and view resources allocated to them. Within a team it is possible to create multiple testbeds by separating them into projects.

4.2 Infrastructure Provisioning

As mentioned above, OpenStack already has all the features required for the infrastructure provisioning module. Namely the OpenStack Heat project makes it possible to define infrastructure using so-called Heat templates. While OpenStack Heat would provide everything we need, we decided to use the infrastructure as code tool Terraform (https://www.terraform.io/) instead, as it supports a wide variety of computing platforms.

Using Terraform, we are able to define complex infrastructure modules which can be reused across multiple testbed configurations.

Due to its infrastructure as code nature it can also version and store our testbed infrastructure definitions using common code versioning systems (e.g., GIT). This modularized infrastructure approach allows us to quickly develop complex testbeds only using a few hundred lines of Terraform code. Figure 2 shows an excerpt of an example configuration that creates three networks and connects a special management host to all three.

```
module "locnet" {
    source = "git@git-service.ait.ac.at:sct-cyberrange/terraform-modules/openstack-fwnet.git"
    network_name = var.locnet_name
    cidr = var.loc_cidr
    fwip = var.loc_gw
    dns = var.loc_dns
    fwimage = var.loc_fwimage
    fwflavor = var.loc_fwflavor
    extnet-id = data.openstack_networking_network_v2.extnet.id
}

module "secnet" {
    source = "git@git-service.ait.ac.at:sct-cyberrange/terraform-modules/openstack-fwnet.git"
    network_name = var.secnet_name
    cidr = var.sec_cidr
    fwip = var.sec_gw
    dns = var.sec_dns
    fwimage = var.loc_fwimage
    fwflavor = var.sec_fwflavor
    extnet-id = module.locnet.network_id
}

module "mgmthost" {
    source = "git@git-service.ait.ac.at:sct-cyberrange/terraform-modules/openstack-mgmthost.git"
    image_id = data.openstack_images_image_v2.image.id
    publicnet-id = data.openstack_networking_network_v2.extnet.id
    network_ids = [module.locnet.network_id,module.secnet.network_id,module.internet.network_id]
}

module "internet" {
    source = "git@git-service.ait.ac.at:sct-cyberrange/terraform-modules/openstack-inet.git"
    router_name = var.router_name
    dnsimage_id = data.openstack_images_image_v2.image.id
}
```

Figure 2: Terraform Network Configuration Example

In Terraform actual infrastructure instances and its code representations are synchronized using the Terraform State. This state can be either stored as a local file or on a remote storage server. The AIT Cyber Range uses a HashiCorp Consul server for remote state storage. States for the various testbeds and their modules are stored in key prefixes relative to the OpenStack domain and project the testbed is instantiated in. This state storage scheme allows us to reuse testbeds across teams and projects without the need to duplicate infrastructure code.

Infrastructure components are assigned labels based on their role within the scenario as part of the testbed configuration. This labeling is achieved by configuring OpenStack compute node metadata as part of the Terraform configuration. The labeling can then be used by the software provisioning module to map machine instances to their roles and apply software configuration accordingly.

4.3 Software Provisioning

The AIT Cyber Range software provisioning module is implemented using the configuration management tool Ansible (https://www.ansible.com/). Ansible provides us with the ability to define software deployment and configuration as templatable code. Similar to Terraform, it also allows us to modularize our Ansible code using Ansible Roles.

Using Ansible Roles we can define software configurations (e.g., for a Postfix server) which can be reused for multiple machines and testbeds. Many members of the Ansible community also provide their Ansible Roles under open source licenses, making it possible for us to integrate their roles as part of cyber range testbeds. Tasks such as the configuration of multiple users on a systems can be achieved in a few lines of Ansible code. Figure 3 shows an example Ansible Playbook used to configure Samba shares vulnerable to SambaCry (CVE-2017-7494).

```
- name: Setup and configure samba shares
  hosts: shares
  become: true
  vars:
    samba_install_version: "4.5.9"
    samba_domain_master: false
    samba_local_master: false
    samba_mitigate_cve_2017_7494: false
    samba_users_dict: {}
    samba_users: "{{ (samba_users_dict | add_usernames(target='name')).values()|list }}"
    user_list_host: "{{ (samba_users_dict | add_usernames(target='name') | encrypt_passwords(hashtype='sha512')).values()|list  }}"
  roles:
    - grog.group
    - role: grog.user
      vars:
          user_createhome: false
          user_shell: /usr/sbin/nologin
    - samba
```

Figure 3: Ansible configuration of vulnerable Samba shares

As mentioned above in the AIT Cyber Range all machines are assigned their roles through metadata labels as part of the Terraform infrastructure configuration. The labels and connection information needed for applying Ansible configuration to the deployed infrastructure is read using the Ansible OpenStack inventory provider. For the software provisioning process we use a special management host which has been configured to be connected to all network zones that are contained within a testbed while also being assigned a public IP from the OpenStack domain's public network. This allows our cyber range to connect to testbed machines without impacting the simulated network and its various zones.

The usage of labels, the OpenStack inventory provider, and the management host allows us to decouple the software provisioning from the actual infrastructure configuration to some degree. Since all the relevant information can be read a runtime, there is no need to know the actual network structure or IP addresses of specific machines in the context of the software provisioning configuration. This allows us to create complex configurations which can be applied to multiple differently structured testbed infrastructures, as long as the contained roles can be mapped to a machine by use of the labeling system.

4.4 Scenario Engine

In the AIT Cyber Range the scenario engine is implemented by our in-house developed GameMaker. The GameMaker, shown in Figure 4, is a web-based application used to control the scenario flow as well as to define and execute injects within the context of a cyber range testbed. The GameMaker is deployed as part of the above mentioned management host during the software provisioning process. It has network access to all systems within a testbed. The current iteration of the AIT Cyber Range GameMaker is still limited in its capabilities and is mostly used to direct non-technical flow of cyber exercises, e.g., participant instructions or predefined non-technical events, such as email communication from a Computer Security Incident Response Team (CSIRT). We are currently in the process of developing our scenario engine further to allow for more complex technical injects, e.g., running fully automated attack chains against a testbed infrastructure.

5 USE CASES

This section summarizes the main use cases of the cyber range.

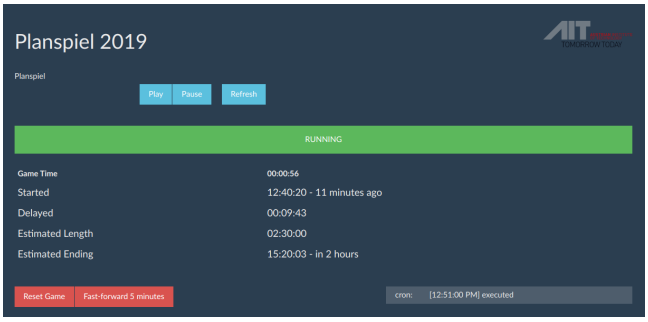

Figure 4: GameMaker Control Panel Screenshot

5.1 Cyber Exercises

Cyber security exercises have become a vehicle to train and test the resilience of organizations and individuals. Cyber security exercises can be structured and designed in various ways (cmp. [6]). The AIT Cyber Range has provided a dynamic, virtual environment for several exercises. In the following, three examples are summarized: First, the *intra-organizational cyber security exercise* focuses on the development of intra-organizational strengths and capabilities of a single organization. The goal is to increase the organizations crisis management, incident response and resilience. The exercise consists of up to 20 participants that work in different departments of the same organization (e.g., IT, Legal, GDPR, Human Resources, IT Security). Second, the aim of a *national, cross-sector cyber security exercise* is to raise awareness and increase the capabilities of several stakeholders (e.g., operators of essential services (OES), public authorities, large organizations, SMEs). The exercise is designed to establish and maintain technical skills and competences, enable cyber security awareness and information sharing (cmp. [13]). Third, the *international, cross-organizational, cross-sector cyber security exercise* focuses on the global challenge of incident response, incident management and information sharing across countries and sectors. This exercise consists of various teams (e.g., SMEs, CSIRTs, OES or public authorities). Together, the teams work on mitigating and minimizing threats and attacks.

With the flexibility of the architecture, the cyber range provides the infrastructure, participant access, technical scenario and injects to host these exercises.

5.2 Training

Additional to cyber security exercises, the cyber range can be set up to host regular training courses for educational purposes. For example, the infrastructure in the cyber range can be set up to reflect the production systems of SMEs or large organizations in various sectors (e.g., IT, energy, manufacturing, finance, healthcare). Often, training content is a combination of a theoretical elaboration and a practical exercise (e.g., hands-on practice). In our experience, this is a very efficient way to adopt new methods or practices. So far, the cyber range has provided a training platform in the following training courses: In the *Information security* course, injects that are used in the cyber security exercises are utilized for e.g., incident response, network security, malware analysis or forensics. These hands-on training courses target specifically professionals, researchers or others who are interested in information security training (cmp. [8]) and improve their dexterity. The *Computer security in industrial control systems* training course provides an overview of industry-specific protocols and technologies. Furthermore, it addresses important aspects of ICS security such as network security, access control or physical security. The cyber range has hosted customized *Industrial training* courses to increase skills and competences of employees in Industry 4.0. These training courses contribute to the skill development of the workforce. The training was developed as an additional way to support the digital transformation of work places.

5.3 Security Research and Development

For research and development, the cyber range (1) is used as testbed to develop and test new approaches and methods (e.g., defense methods) and (2) is the basis for specific cyber range research (e.g., federation, scenario generation, measurement). In the following, two research areas are summarized.

5.3.1 Simulation and Detection of Attacks in Industrial Control Systems. We are using the AIT Cyber Range to support our research activities on computer security incident response and analysis in the nuclear sector. In the project SIREN, for example, several novel technologies are being evaluated that aim to detect the onset of a cyber-attack at a nuclear facility. To support this activity, a representative virtual environment has been configured using our cyber range. This environment consists of several security zones that are used to support facility functions that have different levels of criticality, e.g., from enterprise systems through to those that are being used to control key processes, such as reactor cooling. The implementation of zones is realized through the implementation of virtualized security controls, such as firewalls. The configuration of these zones and the systems within them are described using Ansible scripts that have been defined by partners in the project. In addition to this virtual environment, using the AIT cyber range, we can integrate real industrial equipment, such Programmable Logic Controllers (PLCs) and Human Machine Interfaces (HMIs), which control a simulated model of processes in a nuclear facility. This combination of software and hardware in the loop enables us to perform attacks against representative systems and gain insights into their potential consequences to operational facilities within a plant [1]. The technologies that have been developed for the AIT Cyber Range allow us to rapidly adapt scenarios, to evaluate different security controls, and to use subsets of the environment for demonstration and training.

5.3.2 Evaluation of Intrusion Detection Systems. Most Intrusion detection systems (IDS) are designed, or at least specifically configured, for application in particular environments and focus on the detection of pre-determined attack techniques (cmp. [17]). Accordingly, objective IDS benchmarking for selection and deployment in real world applications is not trivial [20]. For this reason, research groups have developed testbeds that resemble real networks and allow IDS deployment as well as attack execution in controlled environments [16]. Testbeds are essential to validate, evaluate, and

compare the capabilities of IDSs. They offer analysts the opportunity to challenge IDS with a wide variety of attack scenarios, which is the basis for unbiased investigations. Otherwise, it is not possible to reliably assess whether the IDS under test performs with similar efficiency and effectiveness when deployed in productive operation. Another challenge is that most existing testbeds are relatively static, because their configuration relies on manual input and domain knowledge. This prohibits fast instantiation of different testbeds with variable configurations. The AIT Cyber Range applies a model-driven approach and offers the possibility to obtain multiple testbeds with variations, which is highly beneficial for IDS evaluation. More available data representing different technical environments enable the generation of separate training, validation, and test data sets, improve robustness of evaluation results, and support validation of approaches in different application environments.

6 CONCLUSION AND FUTURE WORK

This paper presented design considerations, architecture and implementation of the AIT Cyber Range. The cyber range is a flexible, scalable and virtual environment to support exercises, training and research. In particular, it consists of the building blocks computing platform infrastructure provisioning, software provisioning and scenario engine. With the cyber range, many exercises and training courses have been successfully held. More than 350 participants have joined or competed in one of our exercises or training courses. With this paper, the authors aim to contribute to the overall understanding and information sharing on the design and utilization of cyber ranges. For future work, we aim to investigate the utilization of the cyber range in particular for interoperability and federation of cyber ranges. Furthermore, we will further develop the building blocks to support and conduct even more complex, realistic and dynamic threat scenarios and attacks.

ACKNOWLEDGMENTS

This work was partly funded by two projects: The SIREN project has received funding from the IAEA as part of the CRP J02008 on Enhancing Computer Security Incident Analysis at Nuclear Facilities. The iDev40 project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 783163. The JU receives support from the European Union's Horizon 2020 research and innovation programme. It is co-funded by the consortium members, grants from Austria, Germany, Belgium, Italy, Spain and Romania. The information and results set out in this publication are those of the authors and do not necessarily reflect the opinion of the ECSEL Joint Undertaking.

REFERENCES

[1] David Allison, Paul Smith, Kieran McLaughlin, Fan Zhang, Jamie Coble, and Rodney Busquim. 2020. PLC-based Cyber-Attack Detection: A Last Line of Defence. In *IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts*. IAEA, 10. https://conferences.iaea.org/event/181/contributions/15513/

[2] Agnė Brilingaitė, Linas Bukauskas, and Eduardas Kutka. 2017. Development of an Educational Platform for Cyber Defence Training. In *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 73–81.

[3] Jon Davis and Shane Margath. 2013. *A Survey of Cyber Ranges and Testbeds*. Technical Report DSTO -GD -0771. Cyber Electronic Warfare Division, DSTO Defence Science and Technology Organisation, Edinburgh, South Australia 5111, Australia. http://www.dtic.mil/dtic/tr/fulltext/u2/a594524.pdf

[4] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)*. ACM, Berlin, Germany, 915–928.

[5] ECSO. 2020. *Understanding Cyber Ranges: From Hype to Reality*. WG5 PAPER. European Cyber Security Organisation (ECSO), Brussels, Belgium. 31 pages. https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf

[6] ENISA. 2015. *The 2015 Report on National and International Cyber Security Exercises*. Technical Report 1.0. European Union Agency for Network and Information Security (ENISA)„ Heraklion, Greece. 32 pages. https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises/at_download/fullReport

[7] B. Ferguson, A. Tall, and D. Olsen. 2014. National Cyber Range Overview. In *2014 IEEE Military Communications Conference (MILCOM)*. IEEE, Baltimore, MD, 123–128.

[8] M. Frank, M. Leitner, and T. Pahi. 2017. Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. In *2017 IEEE 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*. IEEE, Orlando, FL, USA, 38–46. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23

[9] Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. 2019. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering* 45, 5 (May 2019), 521–536. https://doi.org/10.1109/TSE.2017.2782813

[10] J. Kim, Y. Maeng, and M. Jang. 2019. Becoming Invisible Hands of National Live-Fire Attack-Defense Cyber Exercise. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. IEEE, Stockholm, Sweden, 77–84.

[11] Stela Kucek and Maria Leitner. 2020. An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. *Journal of Network and Computer Applications* 151 (Feb. 2020), 102470. https://doi.org/10.1016/j.jnca.2019.102470

[12] Stela Kucek and Maria Leitner. 2020. Training the Human-in-the-Loop in Industrial Cyber Ranges. In *Digital Transformation in Semiconductor Manufacturing (Lecture Notes in Electrical Engineering)*, Sophia Keil, Rainer Lasch, Fabian Lindner, and Jacob Lohmer (Eds.). Springer International Publishing, Cham, 107–118. https://doi.org/10.1007/978-3-030-48602-0_10

[13] Maria Leitner, Timea Pahi, and Florian Skopik. 2017. Situational Awareness for Strategic Decision Making on a National Level. In *Collaborative Cyber Threat Intelligence*, Florian Skopik (Ed.). CRC Press, 225–276.

[14] U.S. Department of Commerce National Institute of Standards and Technology. 2018. *Cyber Ranges*. Technical Report. NIST, US. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

[15] Cuong Pham, Dat Tang, Ken-ichi Chinen, and Razvan Beuran. 2016. CyRIS: a cyber range instantiation system for facilitating security training. In *Proceedings of the Seventh Symposium on Information and Communication Technology (SoICT '16)*. ACM, Ho Chi Minh City, Vietnam, 251–258.

[16] Florian Skopik, Giuseppe Settanni, Roman Fiedler, and Ivo Friedberg. 2014. Semi-synthetic data set generation for security software evaluation. In *Proc. of the 12th Annual International Conference on Privacy, Security and Trust*. IEEE, 156–163.

[17] Ciza Thomas, Vishwas Sharma, and N Balakrishnan. 2008. Usefulness of DARPA dataset for intrusion detection system evaluation. In *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008*, Vol. 6973. International Society for Optics and Photonics, SPIE, 164 – 171.

[18] Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupé, Yanick Fratantonio, Luca Invernizzi, Dhilung Kirat, and Yan Shoshitaishvili. 2014. Ten Years of iCTF: The Good, The Bad, and The Ugly. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. USENIX Association, San Diego, CA, 7.

[19] Jan Vykopal, Martin Vizvary, Radek Oslejsek, Pavel Celeda, and Daniel Tovarnak. 2017. Lessons learned from complex hands-on defence exercises in a cyber range. In *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE Computer Society, Indianapolis, IN, USA, 1–8. https://doi.org/10.1109/FIE.2017.8190713

[20] Markus Wurzenberger, Florian Skopik, Giuseppe Settanni, and Wolfgang Scherrer. 2016. Complex log file synthesis for rapid sandbox-benchmarking of security- and computer network analysis tools. *Information Systems* 60 (2016), 13–33.

[21] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. 2020. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security* 88 (Jan. 2020), 101636. https://doi.org/10.1016/j.cose.2019.101636