Building a Cyber Range for training CyberDefense Situation Awareness

Thibault Debatty
Cyber Defence Lab
Royal Military Academy
Belgium
thibault.debatty@rma.ac.be

Wim Mees
Cyber Defence Lab
Royal Military Academy
Belgium
wim.mees@rma.ac.be

***Abstract*—In cyberspace, maintaining a high level of situation awareness (CDSA) is critical for supporting the decision making process. This can only be trained by simulating real incidents as realistically as possible. A Cyber Range is therefore an essential tool. It allows to simulate complex networks and makes it possible to involve large numbers of participants. In this paper we present the important role of Cyber Ranges for improving CDSA, then we present how a Cyber Range can be implemented to allow such a training.**

I. Introduction

In cyberspace, maintaining a high level of situation awareness is critical for supporting the decision making process. A deficient situation awareness leads to suboptimal or sometimes even counterproductive decisions, with inefficient actions slowing down the response to an attack and quick wins being overlooked.

Given the importance of situation awareness in the cyber decision making process, it is important to develop appropriate training methods for developing and evaluating cyber situation awareness in individuals as well as in teams. The evaluation of individual and team cyber situation awareness can also be used for improving system design, evaluating the effectiveness of commercially available solutions when used in the context of an organization's mission critical systems, etc.

A cyber range is a tool that allows to simulate a complete network, and is usually used for cyber training and cybertechnology development. The possibility to simulate large complex networks allows to improve the realism and quality of training and eventually the knowledge, skills and attitudes of cyber specialists. This helps strengthen the stability, security and performance of IT systems used by private companies, governments and military agencies.

It is currently a major research topic [8], [2], with multiple institutions and private companies investing massively: in November 2016, IBM has announced it would invest $200m in Cyber Range facilities [4].

In section II the important role of a cyber range for training cyber defense situation awareness is presented. In section III our implementation of a cyber range is discussed, followed in section IV by a few examples of scenarios that can be instantiated on our cyber range and a brief discussion of how these scenarios aim to improve the trainees' situation awareness.

II. The role of cyber range-based training

A. Cyber Defense Situation Awareness

Given the speed at which events unfold during a cyber incident, a rapid and efficient decision making process is essential. The complexity of managing a cyber operation furthermore requires different specialist working closely together.

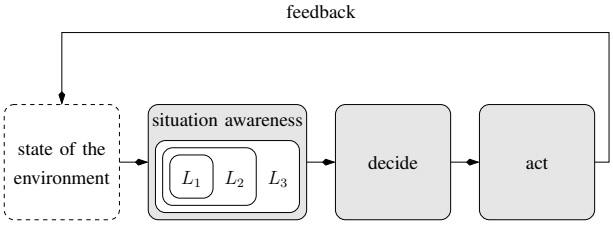

Fig. 1. Endsley's decision making model

In [9] the Boyd and Endsley decision making models have been discussed and the important role of *"Cyber Defense Situation Awareness"* (CDSA) in the decision making process was highlighted. In her decision making model, Endsley [6] defines three levels of *"Situation Awareness"* (SA), as is shown in figure 1:

- level 1 SA *("perception")*: perceive the real-time status, attributes and dynamics of relevant elements in cyberspace. This step involves monitoring the communication network and information systems, receiving security incidents and events as well as end-user reports, detecting anomalies, ... At the level of a *"Security Operations Centre"* (SOC) the level 1 SA is for instance provided by a wall of screens showing the outputs of monitoring and *"Security Incident and Event Management"* (SIEM) tools.
- level 2 SA *("comprehension")*: aggregation and assessment of level 1 information in order to understand how the current situation impacts on our goals and objectives.

This information can for instance be materialized in the form of high-level diagrams showing the outline of a cyber-attack in an intelligence report produced by an analyst.

- level 3 SA *("projection")*: the ability to extrapolate the actions of the elements in cyberspace into the future, based on the L2 comprehension of the current situation and an adequate knowledge of the dynamics of the elements.

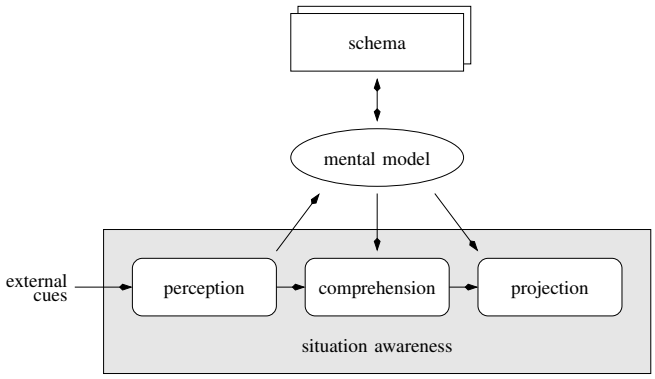

Fig. 2. Mental models and schema

In Endsley's model, situation awareness is achieved using *"mental models"*, as is illustrated in figure 2. Rouse and Morris define mental models as "mechanisms whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future states" [10].

These mental models are built ad hoc by activating one or more *"schemata"*, which are prototypical states of mental models, that make it possible to easily match a perceived situation with a number of well-known and recognized classes of situations, pre-loaded in memory, and as a result provide comprehension and projection as a single step. Endsley furthermore defines the notion of *"scripts"* associated with a schema, which are predefined sequences of actions that define what to do in the cases that are represented by the schema, and therefore allow for very rapid decision making, which is exactly what is needed in cyberspace.

B. Individual CDSA

There are a number of reasons why individual CDSA can be insufficient [7].

- level 1 individual CDSA: the expert fails to correctly perceive the situation in his specific domain of expertise. This can be due to a number of reasons.
  - The information was not available to him.
    This can reveal gaps in the monitoring and detection capabilities of the information systems.
  - The information was available but he did not see it or saw it but then forgot it. This can be due to for instance attention narrowing, task-related or other distractions or excessive workload.
  - The information was observed but misinterpreted. This can for instance be caused by prior expectations that bias the observation.
- level 2 individual CDSA: the expert fails to correctly comprehend the situation.
  This can be caused by:
  - a missing or incomplete mental model, for instance when important configuration changes were performed, a new type of attack is performed, or when the individual lacks experience or thorough training.
  - an incorrect mental model, caused by a lack of formal structured training, exaggerated self-confidence, etc.
  - over-reliance on the default values in the mental model
- level 3 individual CDSA: the expert cannot project the current situation into the future to develop realistic courses of action.
  This is typically also due to lacking or incorrect mental models, or to a tendency to over-project current trends.

When the results from the extensive studies of situation awareness with airline pilots is transposed to cyber operators, the following CDSA performance levels are to be expected. Junior operators will typically focus more on the development and application of their individual technical skills and tend to behave as passive consumers of the immediately available information. As a result they develop mostly L1 SA, and fall short with regard to L2 and L3 SA. More experienced operators also focus on knowing the systems, the incident detection tools and their limits in depth. They actively develop L2 SA and tend to seek out information with that purpose. The most experienced ones will deal with large numbers of details and the complex relationships that exist.

C. Team CDSA

When problems with the combined CDSA of a team is causing problematic decision making, this can be due to a number of causes, for instance the lack of communication between team members or the misinterpretation of the exchanged information. Certain team characteristics were on the other hand found to result in a better team SA that leads to faster problem solving and to a faster detection of new problems that develop.

The first one is demonstrating knowledge of the actions of the other team members. A second one is the habit of verbalizing actions and intentions. Better performing teams also tend to take longer to make decisions because they actively gather more information in order to make better decisions. They plan ahead for actions that will occur during peak workload periods, perform actions they will buy them extra time when needed, and dynamically shift responsibilities between team members when needed.

D. Using a cyber range for training situation awareness

Since situation awareness is built up using mental models, and these models are to a large extent developed and fine-tuned through practice and experience, it is clear that cyber range-based training can be used to improve both individual and team CDSA.

Some typical areas that can be targeted in a cyber range-based training for improving individual CDSA:

- *task management:* the trainee can be interrupted by both task related and non-task related distractions, and submitted to peak workloads in a cyber range training scenario.
  This allows the trainees to develop an active task and information flow management practice, so they can avoid information overload situations where they miss critical information.
- *comprehension:* given the appropriate training scenarios, the trainee can furthermore develop new mental models or improve existing ones, in order to achieve a better L2 SA.
- *projection:* experienced cyber specialists spend a significant amount of time in anticipating possible future events using L3 SA in order to develop and select the most favorable course of action.
  This again can be trained by engineering appropriate training scenarios on a cyber range.

Scenarios for training the higher order cognitive skills needed for developing individual SA will therefore focus on attention sharing, workload management, actively seeking for information, etc. However for these trainings to be effective it is essential that the trainees also receive structured feedback on the quality of their SA.

Training scenarios for improving team CDSA will additionally focus on the following aspects:

- avoiding differences in perception and comprehension between team members by sharing information, goals, and by aligning their mental models.
- developing a habit of verbalizing the information that leads to a decision.
- making sure that the results of a decision are fed back to the team members in order to create a culture where the team members' mental models are constantly improving and becoming more robust.

III. Implementation

We present here our implementation of a Cyber Range for training CDSA. It offers multiple advantages:

- the scenario of an exercise is described in a text format (like yaml or json) to allow easy version control, change detection and exchange;
- the scenario definition allows a variable number of trainees, shuch that the same scenario can be directly reused for an exercise involving 10 or 100 participants;
- the scenario allows to directly use Vagrant images [3] as virtual machines, which gives access to thousands of ready to use images;
- the semantic of the scenario allows extensive configuration of the virtual machines, including complete virtual hardware (number of vCPU, amount of memory, number of network interfaces ...), OS (hostname, network configuration ...) and installed software.

The main components of our Cyber Range implementation are: a hypervisor, a remote desktop gateway and an orchestrator (Figure 3).

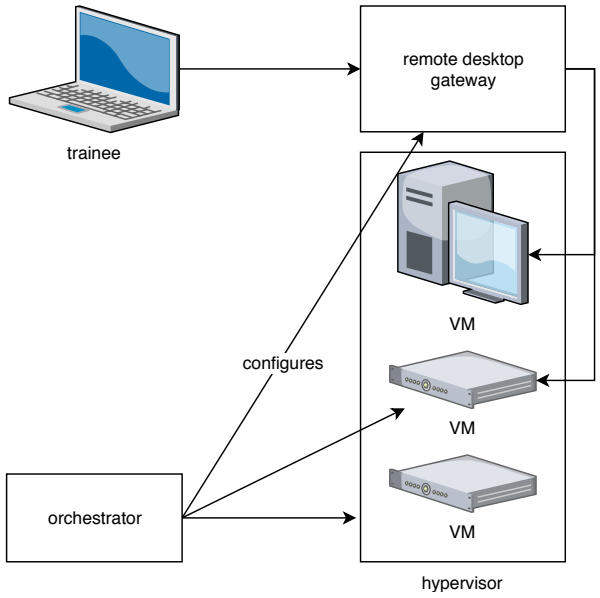

Fig. 3. Architecture of our Cyber Range implementation

The hypervisor is responsible for running the virtual machines (VM) and networks. For cyrange we currently support VirtualBox (which itself relies on KVM/QEMU), although other hypervisors can be supported in the future. The only requirements is that the hypervisor must allow remote desktop access to the virtual machines, either using remote desktop protocol (rdp) or Virtual Network Computing (vnc).

The remote desktop gateway allows the users to connect to the cyber range and use the virtual machines from a browser (Figure 4). We currently use Apache Guacamole [1]. Guacamole is a pure HTML5 gateway that requires no additional plugin (like flash) or client installation. Moreover, it supports both rdp and VNC protocols.

The orchestrator is the main component and the core of the Cyber Range. From the scenario definition, it has to:

- provision the virtual machines:
  - deploy the required images;

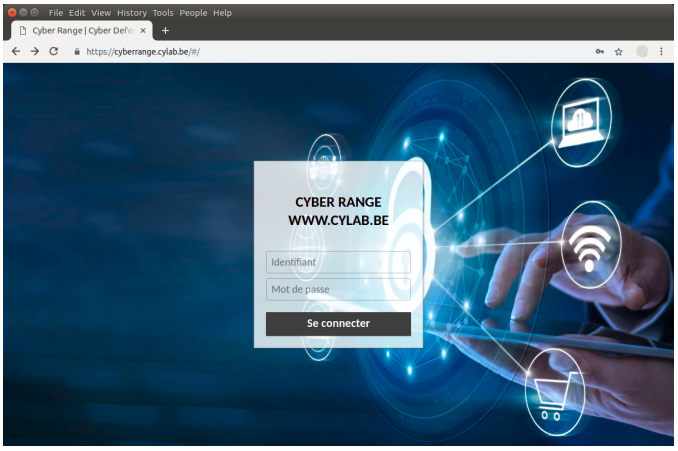

Fig. 4. Login page of the Cyber Range

  - customize the virtual hardware of each VM: number of CPU, amount of memory, number of network interfaces etc.;
  - customize the installed Operating System settings: configure fixed IP addresses, user accounts and passwords etc.;
  - install and configure additional software, like an Intrusion Detection System, a traffic generator, a vulnerable web server, or analysis tools for the trainees' VM for example;
- configure the different virtual networks;
- create the required user accounts in the remote desktop gateway, such that the trainees and trainers can access their assigned virtual machines.

IV. Examples

The semantic of the orchestrator is flexible enough to support the simulation of multiple scenarios. We present here two examples.

A. Web application firewall

In this scenario, all trainees work independently. For each of them we simulate a small 3-tier web architecture consisting of a web application firewall (WAF) and load balancer, two web servers and two database servers. The WAF is responsible for protecting the web application and distributing the load between the two web servers. The actual data is stored on the two database servers to insure performance and reliability.

Each trainee has to configure the different virtual machines to ensure the performance and reliability of the web application, and to protect the web application from attacks that may target possible vulnerabilities left by the application developers.

We typically use this scenario to train the individual CDSA of an operator for the "protect - detect - respond" functions of the NIST cybersecurity framework [5].

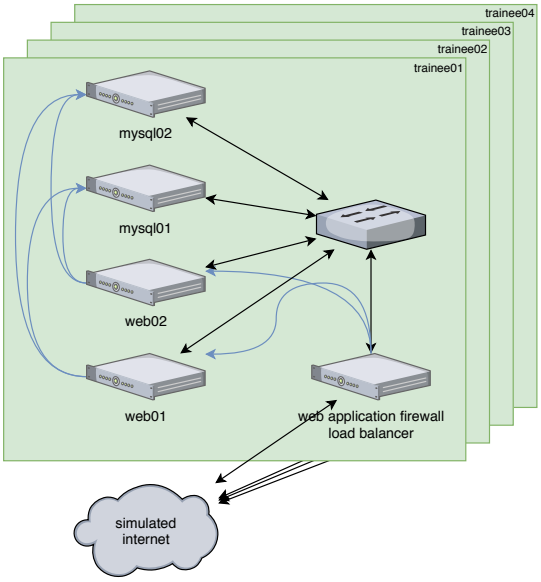

Fig. 5. Web application firewall scenario

We can create distractions and information overload by for instance bombarding the operator with context information, vulnerability reports, etc. We can select unfamiliar configurations for certain components and create attacks the operator is not familiar with, in order to stretch his mental models.

What is important however is to periodically evaluate the different levels of his SA using an objective method, and provide structured feedback to the trainee in order to improve his knowledge, skills and attitudes, and more in particular his mental models.

B. Collaborative scenario

For this scenario, depicted in Figure 6, we simulate a small corporate network. This network consists of a firewall, a DMZ with a honeypot and a vulnerable web server, and an internal network with a few workstations, a security onion server to monitor the network, and a traffic generator. We also create a virtual workstation for each trainee, connected to the internal network.

In the scenario, the attacker manages to compromise an employee workstation using an infected email attachment. The attacker is then able to scan the entire network and hack the web server, from where he steals valuable information including clients credentials and credit card information.

A limited number of trainees, typically consisting of an IT operations staff member, and SOC monitoring operator and a forensics specialist, have to team up to perform the "protect - detect - respond" functions for the whole network.

For this scenario the focus lies on developing team SA, by communicating clearly, verbalizing the collaborative decision

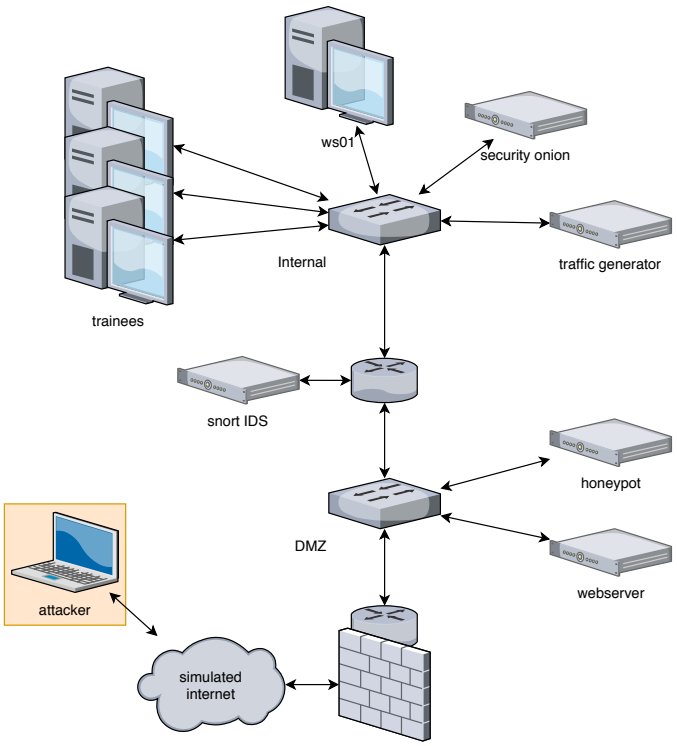

Fig. 6. Simulated collaborative scenario

making process, and learning from the outcome of each decision that is taken and executed.

Again the necessary disruptions will be injected, in the form of information received by the team, requests to report on the situation, external items that are delivered for forensic investigation, etc. The details of the scenario can be made sufficiently subtle and intertwined that an efficient collaboration between the team members is required to discover the mechanisms behind an attack in order to produce the appropriate response.

V. Conclusion and Future Work

In this paper we presented the importance of developing both individual and team Cyber Defence Situation Awareness, and how this skill can be trained using a Cyber Range.

Our implementation can obviously be improved, for example:

- to support other hypervisors like VMware or Hyper-V.
- to support connection with other cyber ranges.
- to allow the scripted simulation of events and attacks.
- to implement less intrusive SA evaluation methods that limit the impact of the evaluation on the normal work-flow.

References

[1] Apache guacamole™. https://guacamole.apache.org/. (Accessed on 02/11/2019).

[2] Cyber ranges: The (r)evolution in cybersecurity training. https://www.slideshare.net/Minsait/cyber-ranges-the-revolution-in-cybersecurity-training. (Accessed on 01/30/2019).

[3] Discover vagrant boxes - vagrant cloud. https://app.vagrantup.com/boxes/search. (Accessed on 02/11/2019).

[4] Ibm spends $200m on cyber range -. https://www.enterprisetimes.co.uk/2016/11/17/ibm-spends-200m-cyber-range/. (Accessed on 01/30/2019).

[5] Matthew P Barrett. Framework for improving critical infrastructure cybersecurity version 1.1. Technical report, 2018.

[6] Mica R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1):32–64, 1995.

[7] Mica R Endsley and Michelle M Robertson. Training for situation awareness in individuals and teams. *Situation awareness analysis and measurement*, pages 349–366, 2000.

[8] Jorge Lopez Hernandez-Ardieta. Keynote speaker 2: Cyber ranges: The (r)evolution in cybersecurity training. In *11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, Barcelona, Spain, December 5-7, 2016*, pages 16–17. IEEE, 2016.

[9] Wim Mees and Thibault Debatty. An attempt at defining cyberdefense situation awareness in the context of command & control. In *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*, pages 1–9. IEEE, 2015.

[10] William B Rouse and Nancy M Morris. On looking into the black box: Prospects and limits in the search for mental models. *Psychological bulletin*, 100(3):349, 1986.

Appendix

Below is a snippet of the JSON definition for the collaboration exercise. It shows multiple advantages of our Cyber Range implementation:

- the number of trainees can easily be modified (line 4);
- new machines can easily be added using existing Vagrant images (line 8);
- the remote desktop gateway is automatically configured as needed (line 14);
- all network interfaces of the virtual machines can be configured using static ip addresses or dhcp (line 40);
- additional software can be installed and configured using Ansible playbooks or some other configuration management tool (line 26).

```
1  {
2    "name": "collaboration",
3
4    "instances": 20,
5
6    "machines": [
7      { "name":  "trainee",
8        "image": "vagrant:cylab/ubuntu-desktop",
9        "networks": [
10         { "mode": "internal",
11           "network_name": "intranet"}
12       ],
13       "playbook": "trainee_playbook.yml",
14       "remote_desktop": true}
15   ],
16
17   "extra_machines": [
18     { "name":  "honeypot",
19       "image": "vagrant:cylab/ubuntu-server",
20       "networks": [
21         { "mode": "internal",
22           "network_name": "dmz",
23           "address": "192.168.1.155",
24           "mask": "255.255.255.0"}
25       ],
```

```
      "playbook": "playbook_honeypot.yml"},

    { "name":  "web server",
      "image": "vagrant:cylab/ubuntu-server",
      "networks": [
        { "mode": "internal",
          "network_name": "dmz",
          "address": "192.168.1.10",
          "mask": "255.255.255.0"}
      ],
      "playbook": "playbook_srv01.yml"},

    { "name":  "router01",
      "image": "vagrant:cylab/ubuntu-server",
      "networks": [
        { "mode": "bridged",
          "bridge_interface": "eno1"},
        { "mode": "internal",
          "network_name": "dmz",
          "address": "192.168.1.1",
          "mask": "255.255.255.0"}
      ],
      "playbook": "playbook_router01.yml"}
  ],

  "dhcp_servers": [
    { "network_name": "intranet",
      "ip": "192.168.0.2",
      "netmask": "255.255.255.0",
      "from": "192.168.0.100",
      "to": "192.168.0.200"}
  ],
}
```