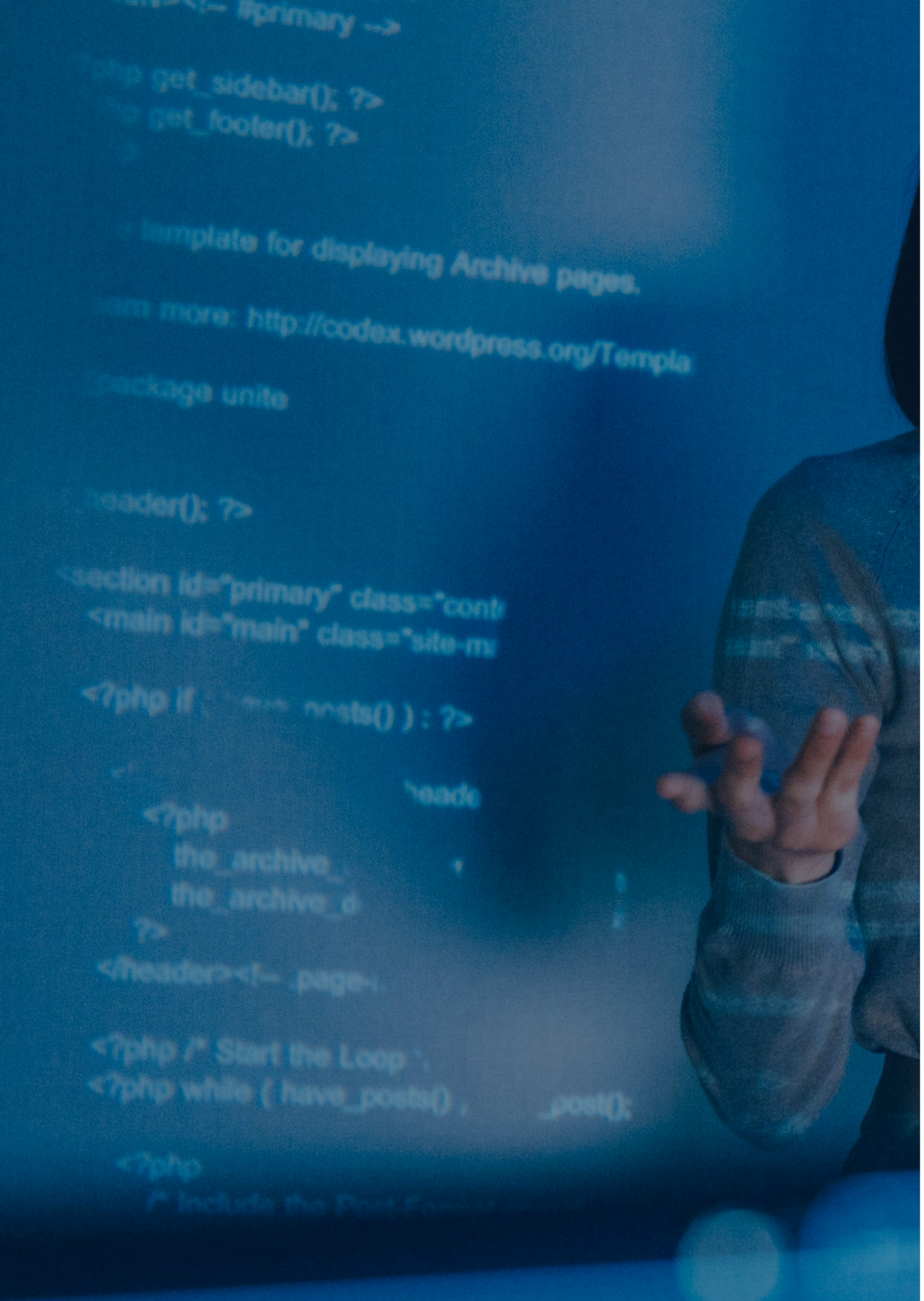
Protelion Cyber Range Platform

Elevating Your Cybersecurity Training

2025



Introduction

In today's digital world, cyber threats are evolving rapidly, making it essential for organizations to stay ahead of potential attacks. Traditional cybersecurity training methods often rely on theoretical knowledge, which does not fully prepare professionals for real-world scenarios. To bridge this gap, Protelion has developed its Cyber Range Platform — an advanced educational and training solution designed to simulate real cyberattacks in a controlled environment. By providing hands-on experience, our platform enhances cybersecurity skills and ensures that professionals are well-equipped to handle modern threats effectively.

The Current Problem

With cyberattacks becoming more frequent and sophisticated, many organizations struggle to find effective ways to train their employees and security teams. The challenges include:

- **Limited access to hands-on training**
  Many institutions provide theoretical cybersecurity education, but practical training is often lacking
- **Lack of teamwork in security operations**
  Cybersecurity is a team effort, yet most training programs focus on individual skill development rather than collaboration
- **Difficulty to replicate real attack scenarios**
  Without realistic simulations, professionals are unprepared for the unpredictability of real-world cyber threats
- **Growing demand for skilled cybersecurity professionals**
  Organizations need specialists who can detect, respond to, and mitigate attacks efficiently
- **Absence of integrated tools for collaborative learning**
  Most platforms do not support realistic, team-based response exercises

> "Cyberattacks are no longer a question of "if", but "when". Yet, many organizations still rely on outdated, theoretical training that leaves teams unprepared for real-world threats."

What We Offer?

To address these challenges, Protelion has developed the Cyber Range Platform — an interactive and scalable training environment that provides cybersecurity professionals, students, and organizations with practical experience in handling cyber threats. Our platform allows users to engage in real-world attack simulations, helping them develop the critical skills needed to secure digital infrastructures. It supports both individual and team-based exercises, allowing flexible training delivery to suit different organizational needs. The platform also features a no-code scenario editor and a library of ready-to-use templates, enabling quick and easy customization of training exercises.

What is Cyber Range?

Protelion Cyber Range is an advanced educational platform designed to simulate real-world cyberattacks in a safe and controlled environment. It models a typical corporate network infrastructure through virtual machines, enabling participants to practice detecting, mitigating, and responding to cyber threats. By offering structured training exercises, our Cyber Range helps improve cybersecurity readiness at all levels — from beginners to experienced professionals.

Training scenarios are built around the so-called vulnerable nodes — virtual machines with vulnerable operating systems and software. Each virtual machine has a set of vulnerabilities and payloads built in. Since the cyber range provides a huge set of well-known vulnerabilities including CVEs from 2023, 2024, 2025, the platform delivers a highly realistic and effective learning experience.

Cyber Range Platform

Key Benefits of Cyber Range

- **Realistic Cyberattack Simulations**
  Train using real-world attack scenarios
- **Hands-on Training**
  Gain practical experience in a controlled environment
- **Customizable Scenarios**
  Adapt training exercises to match organizational needs
- **Collaborative Team-Based Training**
  Enhance teamwork and coordination in cybersecurity operations
- **Integration with Security Tools**
  Practice using industry-standard cybersecurity solutions
- **Flexible Deployment**
  Available as an on-premise or cloud-based solution
- **Defined User Roles**
  Structured responsibilities for training management and participation
- **Continuous Content Updates**
  Includes new vulnerabilities, templates, and support materials

How It Works?

Protelion Cyber Range provides an immersive learning experience through structured training formats, customizable scenarios, and real-time attack simulations. The platform operates as follows:

1. **Simulated Cyber Environments**
   Our platform replicates realistic IT infrastructures using virtual machines, allowing participants to experience cyberattacks firsthand. The simulations include various attack techniques, vulnerabilities, and threat actors to mimic real-world challenges.

2. **Training Formats**
   The Cyber Range offers multiple training formats, including group training formats such as Blue Team (SOC simulation), CSIRT (incident response), Red Team (penetration testing, infrastructure security assessment), and individual such as OSINT (information security awareness and open-source intelligence gathering).

3. **Scenarios**
   Scenarios define specific actions and modifications within the infrastructure. Users can either utilize pre-configured, automated attack scenarios or design their own, based on the vulnerable nodes that we, as the vendor, have added to the platform.

4. **Protection systems**
   The platform integrates real-time monitoring and analytical tools to detect attacks and conduct an in-depth analysis of the virtual hacker's actions. The information gathered from these systems can be used to implement protective measures on the infrastructure and eliminate the consequences of cyberattack.

A typical training session includes defined roles, such as Teacher and Trainee. The teacher does not need any special skills to launch training sessions — it is done via a few clicks. A scenario launches via a web interface, real-time infrastructure deployment, and once the virtual infrastructure is deployed, the training begins. It is a safe environment and even if a trainee damages the infrastructure, the training can easily be redeployed. Upon training completion, the virtual infrastructure automatically shuts down, releasing any allocated disk space.

Depending on the training format, participants are evaluated based on task completion, vulnerability identification, incident response effectiveness, and other relevant criteria — making it well-suited for grading in educational environments.

Cyber Range Platform

Who Can Benefit from Cyber Range?

Protelion Cyber Range is designed for a wide range of users, including:

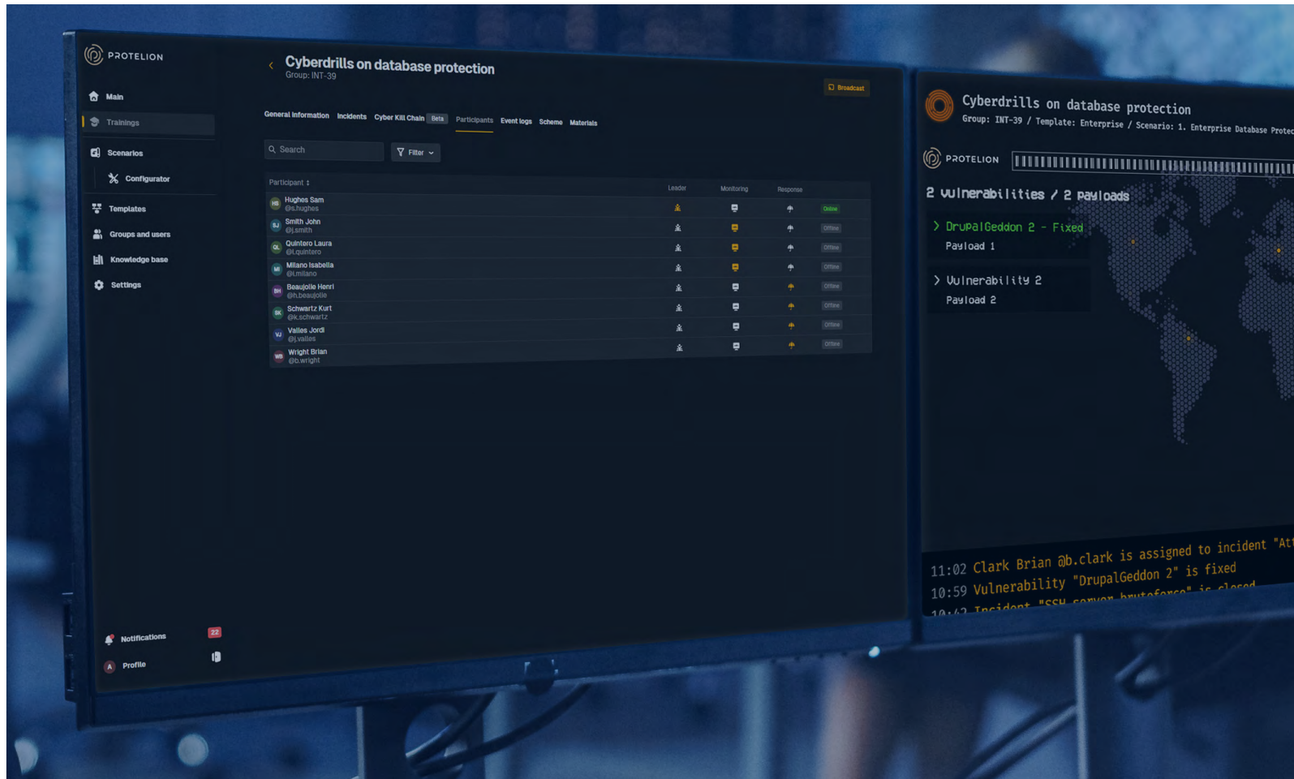
- **Educational Institutions**
  Universities, colleges, and technical schools can integrate Cyber Range into their cybersecurity curriculum to provide hands-on training on a daily basis

- **Enterprise Security Teams**
  IT and security professionals can refine their skills and test incident response strategies in a risk-free environment

- **Government Agencies**
  Defense and intelligence teams can practice handling cyber threats and protecting national security infrastructure

- **Industrial & Corporate Sectors**
  Companies across various industries can train employees to identify and mitigate cybersecurity risks

- **Security Operations Centers (SOC)**
  Teams can simulate end-to-end attack response using actual monitoring tools integrated within the Cyber Range infrastructure



Use Case – Technical University

- Protelion is used in a number of technical disciplines as part of labs.
- Students practice interaction with vulnerabilities and payloads during these labs.
- The teachers use different training formats (Blue Team, Red Team and others) to show cyberattacks from different angles.
- The success of students influences on their final grade in the subject.
- Protelion is also used in various public events.
- Protelion is hosted on-premise and the university has a dedicated class with the workstations and server.

What Value Does it Bring?

For teachers, Protelion serves as a practical extension of their lectures, helping them illustrate theoretical content through real examples.
For students, it provides the opportunity to observe and engage with real cyberattacks in a safe environment, deepening their understanding of the information security domain.

Scenario Example – Enterprise Database Protection

An attacker finds a vulnerability on the company's public website and uses it to gain access to an internal server. From there, the attacker moves further inside the network, targeting an employee's workstation. Their ultimate goal is to steal the company's database.

Attack Steps

1. Exploits a vulnerability on the public website.
2. Gains access to an internal server via this vulnerability.
3. Infects an employee's workstation through a malicious file.
4. Moves laterally through the network to access the database server.
5. Dumps the corporate database.

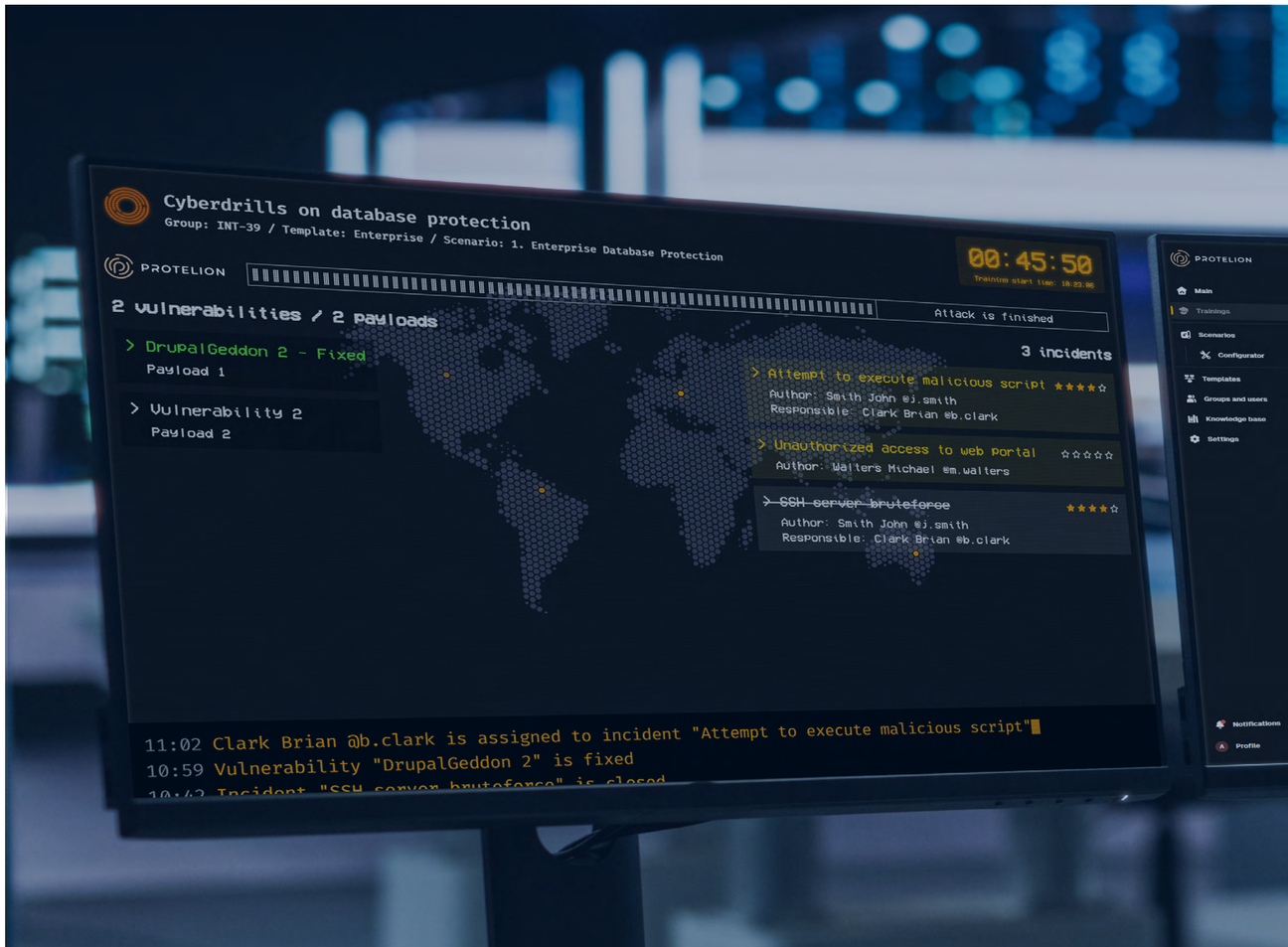
Cyber Range Platform

What Should Participants Do?

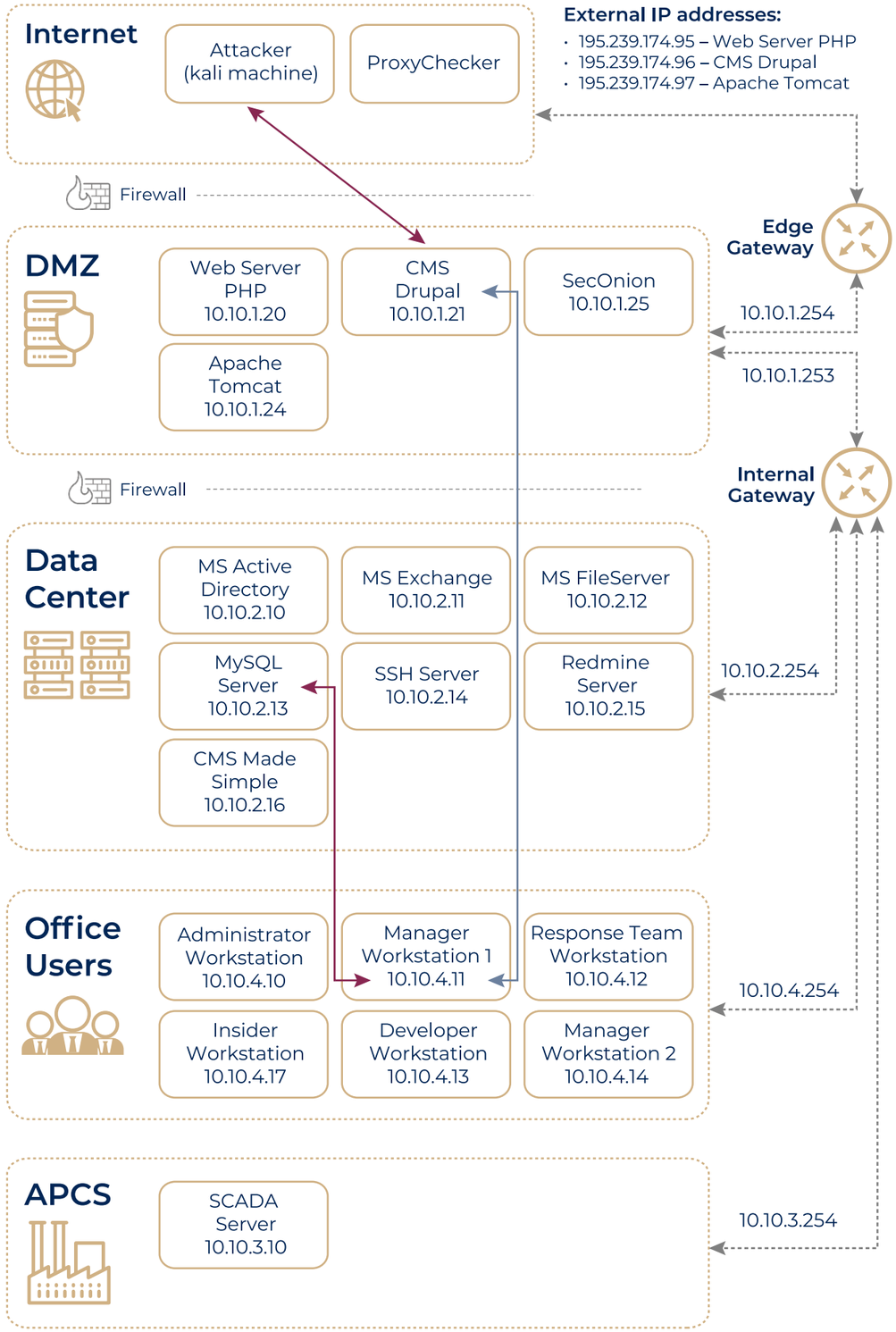
The Monitoring Team must detect the key attack steps using monitoring tools and report any suspicious activity, such as exploitation of vulnerabilities or unusual network behavior, to the Response Team.

The Response Team must fix the vulnerabilities, stop the attacker's access, and take necessary actions to strengthen security and prevent future incidents.

Through this exercise, participants improve their ability to detect and respond to real-world cyberattacks. It strengthens their skills in identifying vulnerabilities, monitoring suspicious activities, and applying appropriate response measures to protect critical data assets. And this is just one example — with Protelion Cyber Range, it is possible to create multiple custom scenarios tailored to a company's specific training needs, threat models, and skill levels.



Scenario Scheme



PROTELION

Oberwallstr. 24
D-10117 Berlin,
Germany

+49 30 206 43 66-0

info@protelion.com

protelion.com

P.CRP.25_v01_BrEng