BV TECH S.p.A.

3 GIUGNO 2024

CYBER RANGE

BV·TECH

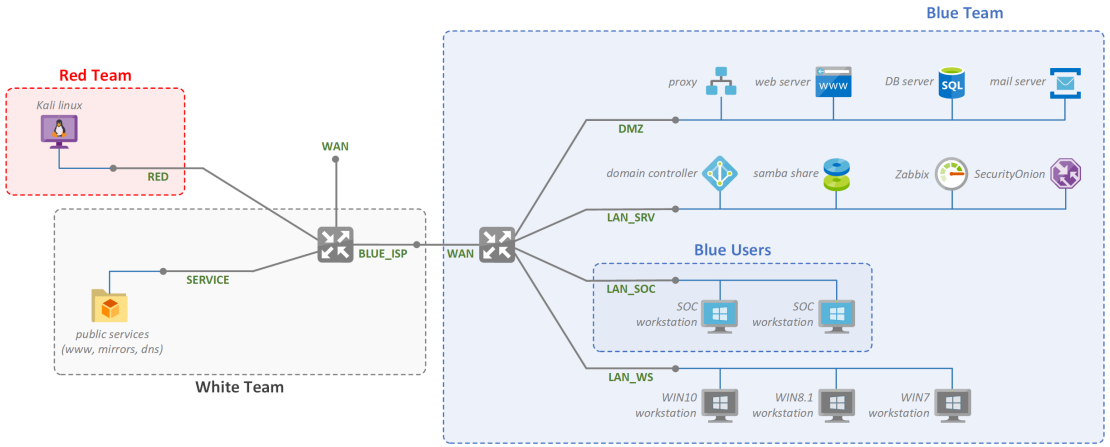
IL CYBER RANGE

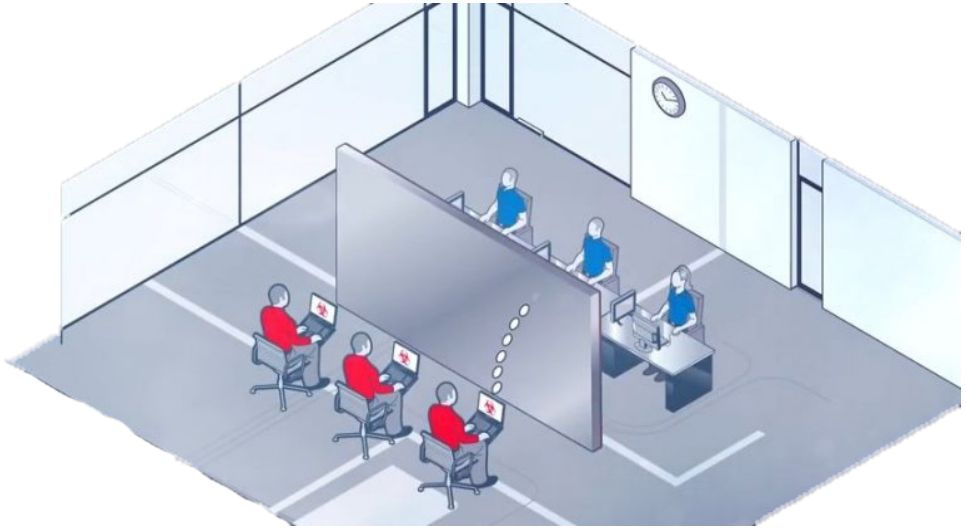
- Un Cyber Range è un'**infrastruttura hardware e software** realizzata per consentire di replicare, in modo **virtuale**, una infrastruttura ICT **reale** (applicazioni, client, server, apparati di rete, sistemi ICS ecc.).
- All'interno del Cyber Range è possibile **simulare**, sull'infrastruttura replicata, **attacchi di natura cyber** all'interno di uno ambiente protetto e circoscritto ma di complessità reale, **senza interferire** con l'ambiente reale.
- Il Cyber Range consente di svolgere attività di **formazione specializzata** ed **altamente realistica** sia per i componenti dei team di sicurezza (Blue) che per quelli di attacco (Red).
- Il Cyber Range è anche un componente indispensabile per svolgere tutta una serie di attività di **sperimentazione e test** in ambito cybersecurity.
- I Cyber Range differiscono tra loro in termini di **caratteristiche funzionali** e **prestazionali**: alcune caratteristiche importanti sono rappresentate dalla possibilità di **integrazione di componenti fisici** negli scenari virtuali («ibridi»), dalle modalità di **creazione e configurazione** degli scenari, dalla possibilità di integrazione con sistemi di **modellazione di processo** (ICS/OT), dal livello di **automazione e realismo** ecc.

CYBER RANGE – FORMAZIONE E ADDESTRAMENTO

In questo contesto il Cyber Range viene utilizzato per eseguire **simulazioni** di **attacco e difesa cyber** su scenari:

- **realistici** (traffico simulato)
- implementati mediante **ambienti virtuali modellizzati**
- **configurati** per lo specifico obbiettivo addestrativo





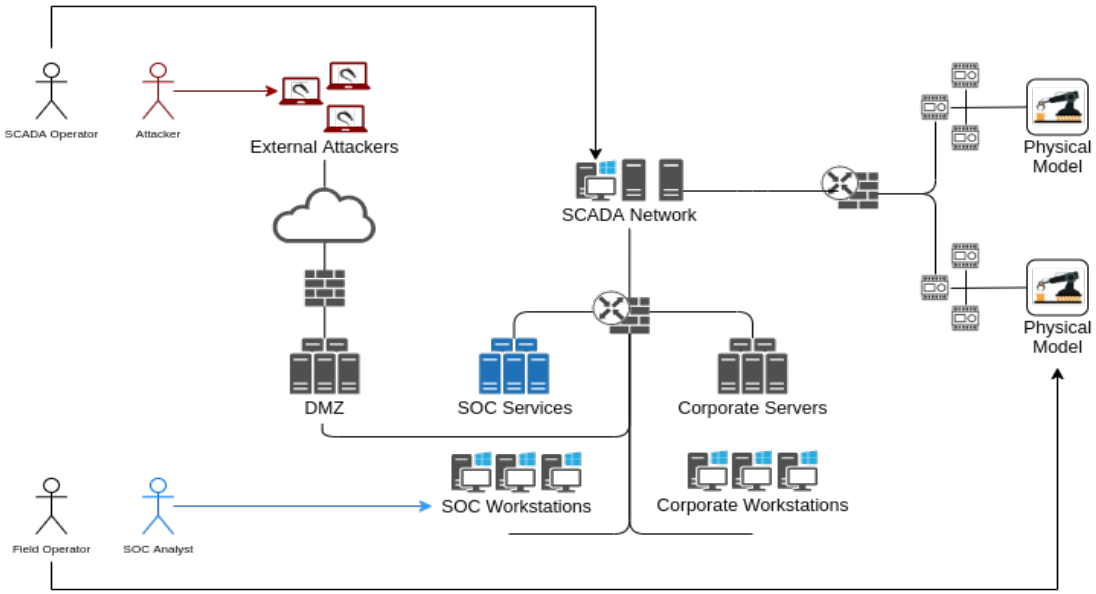
Obiettivi di queste attività sono:

- **formazione** per apprendere le tecniche di attacco o difesa
- **verifica** della gestione e risposta di una squadra in caso di attacco
- **valutazione** delle competenze
- **competizione** attacco/difesa per team building o eventi ***CTF***

CYBER RANGE – SPERIMENTAZIONE E TEST

In questo contesto il Cyber Range viene utilizzato per eseguire **simulazioni** di **attacco e difesa cyber** su scenari:

- **reali** (replica totale o parziale)
- implementati mediante **ambienti ibridi** (se necessario)
- **alimentati da dati reali,** nei c.d. «digital twin»
- per **casi di test specifici** (es. nuove vulnerabilità)

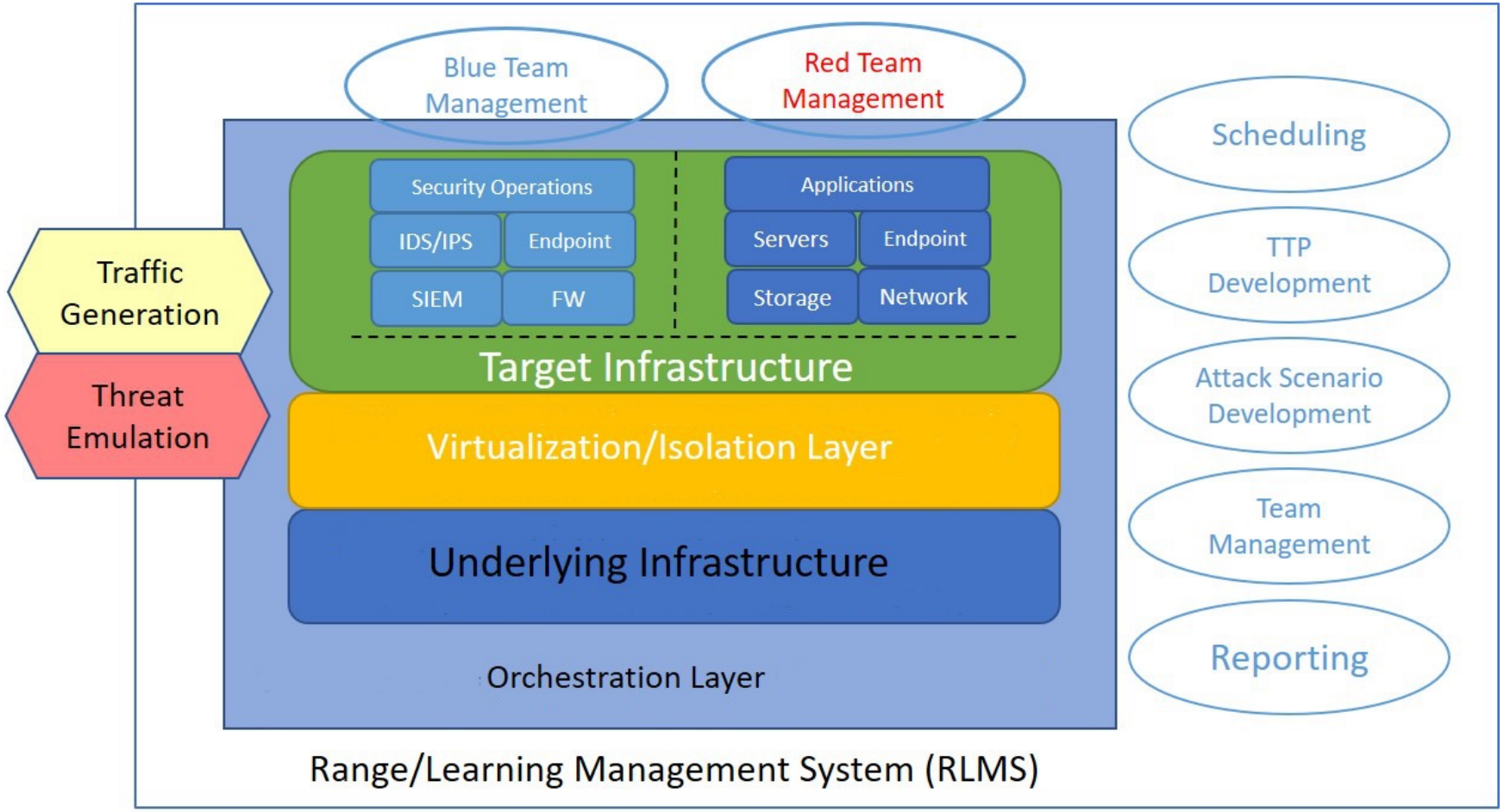


Obiettivi di queste attività sono:

- **valutare** la superficie di attacco a disposizione di un aggressore reale
- **studiare e testare** tipologie di attacco aggressive
- **valutare** l'efficacia degli strumenti e delle metodologie di difesa
- **progettare** nuove tattiche di contrasto alle minacce

ARCHITETTURA

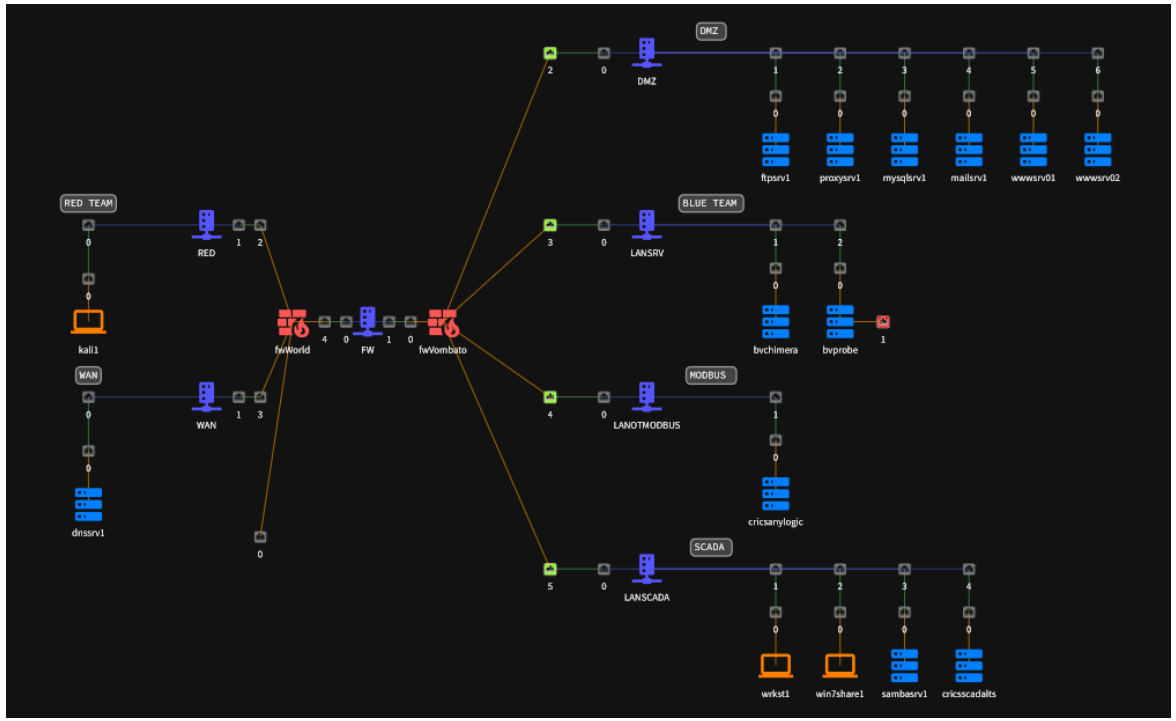
Il Cyber Range è un **ecosistema complesso** costituito da componenti **specializzati** e fortemente **integrati**



CYBER RANGE – LO SCENARIO

Lo scenario rappresenta il **progetto** di una rete virtualizzata. Il Cyber Range si caratterizza per il livello di sofisticazione che offre in termini di

- creazione di **scenari** realistici e rappresentativi
  - Architettura, servizi e protocolli standard e adottati nel settore di riferimento
  - Possibilità di *personalizzazione*
    - Topologia di rete
    - Numero di nodi
    - Tipologia di sistemi (Unix, Windows)
  - Strumenti di attacco e difesa
    - Standard *de facto* (e.g., Kali Linux, OpenVAS, Metasploit)
    - Proprietari (NGFW, NIDPS, SIEM ecc.) o di terze parti
- integrazione con sistemi di modellazione di processo
- automazione del traffico e degli attacchi



Gli Scenari creati possono essere raccolti in **teatri** e possono essere **istanziati** diverse volte, anche contemporaneamente, pur rimanendo **isolati**.

CYBER RANGE BV TECH – CARATTERISTICHE PRINCIPALI

- Accesso alla piattaforma e alle macchine virtuali tramite web **browser**
  - **Team di attacco (Red Team)**
  - **Team di difesa (Blue Team)**
  - **Team di gestione e supervisione**
- **Integrazione** con sistemi di sicurezza proprietari e/o terzi
  - NGFW
  - NIDPS
  - SIEM
- **Integrazione** con componenti fisici esterni **(Cyber Range ibrido)**
- **Integrazione** con sistema di **modellazione di processo** per scenari **ICS/SCADA/IoT**
- **Interfaccia grafica** di configurazione scenari
- **Generatore** automatico di traffico legittimo/malevolo
- **Monitoraggio completo** del traffico di rete
  - Per alimentare i sistemi di difesa e controllo *virtuali*
  - Per monitorare l'operatività *complessiva*
- **Monitoraggio** di dettaglio delle attività **Red** team (keylogging)

CYBER RANGE - RICERCA BV TECH: PUBBLICAZIONI

- Shaharyar Khan**, Alberto Volpatto*, Geet Kalra, Jonathan Esteban**, Tommaso Pescanoce*, Sabino Caporusso*, Michael Siegel**, **“Cyber Range for Industrial Control Systems (CR-ICS) for Simulating Attack Scenarios”**. *Proceedings of the 5th Italian Conference on Cybersecurity (ITASEC21),* 2021, 2940, pp. 246-259.

- Alessandro Santorsola*, Aldo Migliau*, Sabino Caporusso*, **“Reinforcement Learning Agents for Simulating Normal and Malicious Actions in Cyber Range Scenarios”**. *Proceedings of the 6th Italian Conference on Cybersecurity (ITASEC22),* 2022, 3260, pp. 1-16.

- Alessandro Santorsola*, Antonio Maci*, Piero Delvecchio*, Antonio Coscia**, “A Reinforcement-Learning-based Agent to discover Safety-Critical States in Smart Grid Environments”**, *3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Tenerife, Canary Islands, Spain 19-21 July 2023, doi: 10.1109/ICECCME57830.2023.10252540.

* = BV TECH ** = MIT - Sloan