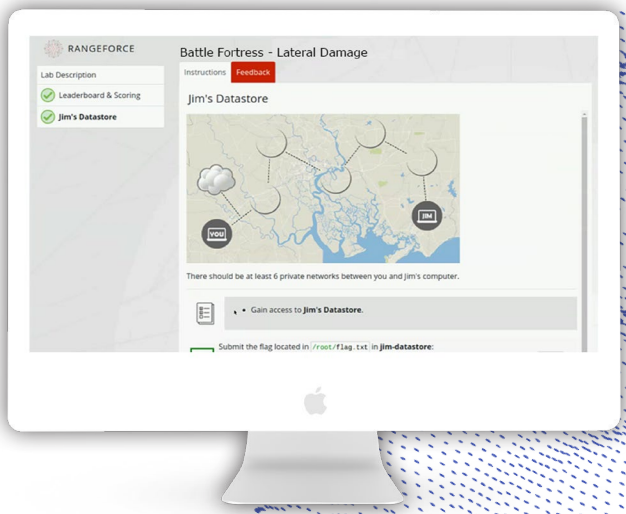
RANGEFORCE

RangeForce Battle Fortress Cyber Range

Hyper-scalable cloud based cyber range delivers affordable, reusable red and blue team exercises

RangeForce Battle Fortress is a hyper-scalable cloud-based cyber range that enables the execution of red/blue team exercises in a realistic environment. Battle Fortress recreates an entire IT environment, emulates existing security tools, and uses real malware and vulnerabilities. Battle exercises are prebuilt blue and red team exercise that can be reused to help deliver valuable training while eliminating the cost and resources required to develop new scenarios.

Defensive (blue-team) or offensive (red-team) online battle exercises are created specifically for security operations and forensic analysts, penetration testers, and application security engineers. Participants gain first-hand offensive and defensive security experience against sophisticated threats in a real-life environment for which there is no substitute.



Develop teamwork: Battle Fortress empowers security teams to train together while acting in their roles to build stronger communications skills and team coordination.

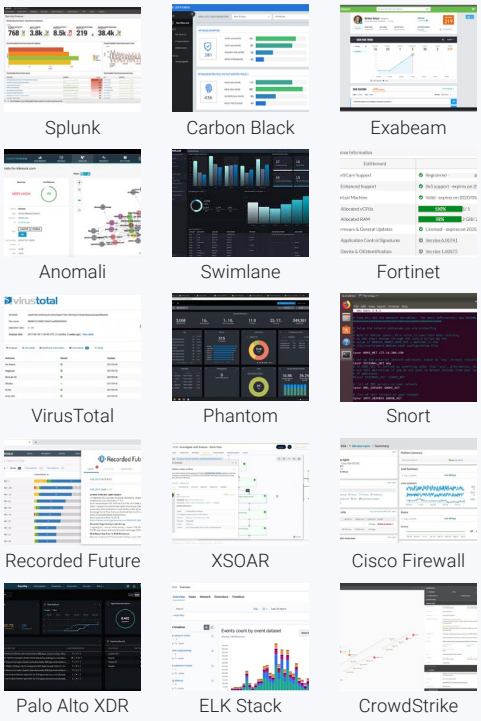
Refine incident response workflows: Practice detection and response processes in real time against real attacks to increase response speed and accuracy.

Continuous training: Post exercise results, define operational weaknesses, playbook limitations, communications issues and individual skills gaps. Post exercise debriefings, define areas for improvement and use RangeForce learning paths to address skills gaps and deficiencies.

info@rangeforce.com www.rangeforce.com (877) 716-4342

Battle Fortress Security Stack Emulation

With Battle Fortress emulation, you use your own security stack for blue or red team exercises. **Our library includes the following tools and more:**

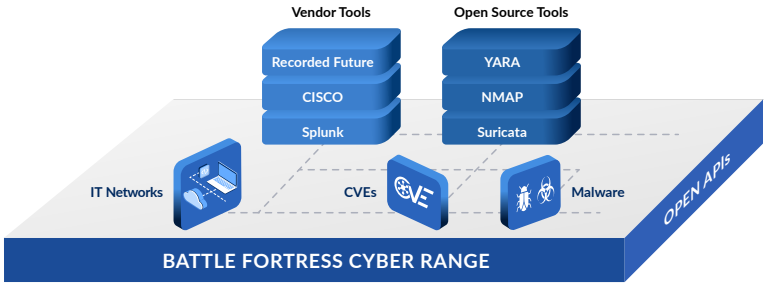


Battle Fortress Architecture

The Battle Fortress Cyber Range and battle exercises can be purchased, deployed, and operated as part of the overall RangeForce CyberSkills Platform or separately. The Battle Fortress cyber range consists of multiple virtual environments that operate together to create infrastructure and scenarios that create a blue or red team exercise.

Fast and easy to deploy: Battle Fortress's cloud based emulation environment and highly scalable virtual architecture makes it easy to create and spin up advanced blue/red team exercises.

Realistic: Battle Fortress features real malware, vulnerabilities, infrastructure, and users all in real-time. Powerful emulation capabilities means your team trains on your security stack in similar IT environments defending against real-world attacks.



How A Battle Exercise Works

Battle Fortress virtual servers recreate realistic training environments with malware and vulnerabilities. Software tool emulators bring vendor security stacks to life. Attack scenarios are unleashed on the exercise participants, who must work together to detect, contain, and remediate the attack.

1. Malware is delivered to Workstation 1 via email.

2. The malware discovers the database and begins exfiltrating "customer data" to the C2 server.

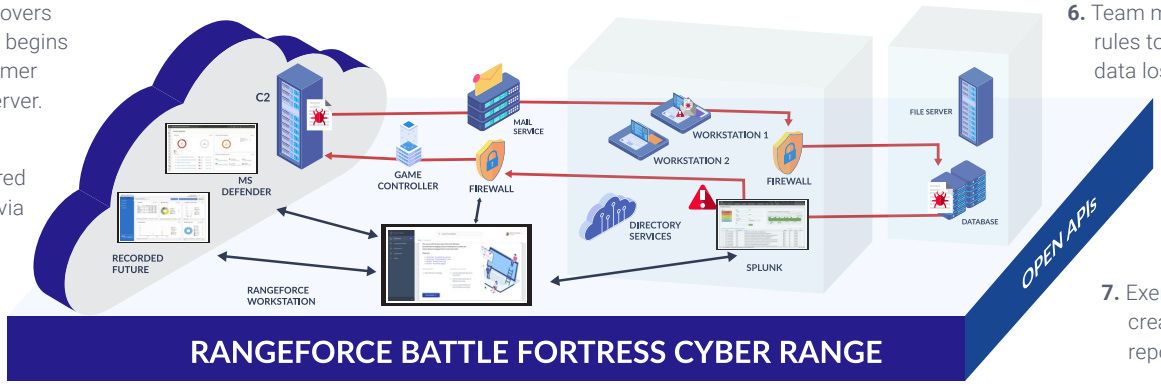
3. The learners must investigate the SIEM alert to find the user and source host.

4. Using EDR, they find artifacts that serve as IOCs.

5. With threat intel to support them, they must determine which host is infected and isolate it.

6. Team must write firewall rules to prevent further data loss.

7. Exercise ends with team creation of an incident report.



info@rangeforce.com www.rangeforce.com (877) 716-4342