RANGEFORCE

RangeForce Battle Fortress

Build team cyber readiness with realistic cyber range training

RangeForce prepares your team to defend against complicated threats before they happen in the real world. With extensive configurability and customization, RangeForce can replicate your existing IT infrastructure and security stack to create an optimal training ground for your team.

Each exercise can be designed to match your team's specific training needs, drawing from a library of available threat scenarios and security solutions. When the exercise begins, your team is tasked with detecting and containing the threat at hand.

The result is highly impactful, on-demand training experiences for your whole team – more accessible and affordable than alternative cyber range solutions.

Security Stack Emulation

- QRadar
- Sysmon
- Fortinet
- SentinelOne
- Carbon Black
- Cisco Firepower
- Phantom
- VirusTotal
- Cisco ASA
- ...and more

Execute realistic team exercises in virtual environments that reflect the real world.

What To Expect

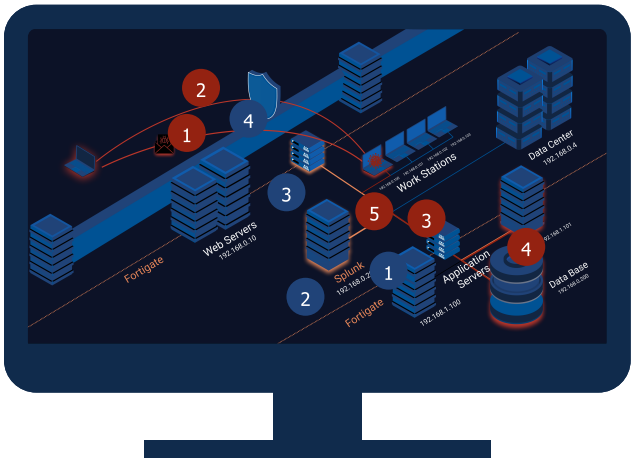
- **Configure your security stack.**
  - Build an emulated replica of your environment with both vendor and open-source security tools.
- **Choose a threat scenario.**
  - Determine which threat your team will be facing during their exercise. Choose from a library of available scenarios, including web defacement, data exfiltration, ransomware, and more.
- **Execute your cyber range exercise.**
  - Experience multi-hour events where your team's communication and cooperation will be put to the test.
- **Review post-exercise team results.**
  - Debrief with RangeForce engineers to understand your team's performance.
- **Build a targeted follow-up training plan.**
  - Follow post-exercise recommendations to build a targeted training program for your team using the RangeForce Battle Skills platform.

RANGEFORCE

Cyber Exercise In Action

1. Adversary delivers a spear phishing attack. Infects a workstation with a malware backdoor.
2. Malware executes, take over the workstation and calls back to the C2 machine.
3. Adversary takes control of the machine, works to escalate privileges.
4. Adversary is able to dump local credentials and begin lateral movement
5. Credentials are used to access files shares and databases. Files are moved for exfiltration.

1. Sensors and logs capture IOCs, and Blue Team SIEM operator receives first set of alerts.
2. Alerts are sent out; response playbooks begin executing.
3. Blue Team must find and correlate multiple IOCs to recognize exfiltration events, identify C2 attack vector.
4. Blue Team defeats attack by deploying firewall rule changes, and identifying and isolating infected machine.



Product Features

- **Real world threats**
  Build an exercise specific to your team's working environment. Defend against threats taken right from the headlines to train together, as a team.

- **Safe and scalable environments**
  Safely train in isolated, cloud-based environments. Access cyber range exercises remotely or in-person, using only an internet browser.

- **Continuous improvement and security orchestration**
  Evaluate your existing cybersecurity processes to better coordinate team operations. Train your team to use the right tools at the right time with increased security orchestration.

- **RangeForce training ecosystem**
  Utilize post exercise results to identify skills gaps. Prepare your team for its next cyber range exercise, choosing from hundreds of RangeForce training modules.