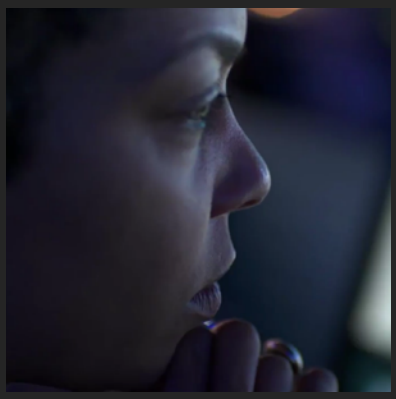
You’re under attack. Now live the response.

Train with an elite squad of cyber first-responders, in a premier security training ground. Get the IBM X-Force Command Experience.



It’s the premier cybersecurity training experience. Where the best military and intelligence agencies, banks and energy companies in the world bring their teams to prepare for the un-predictable and respond to do-or-die situations after a security breach. The IBM X-Force Command Experience helps you prepare for worst-case scenarios with intense, gamified drills based on real-world attacks, led by X-Force Command experts who have first-hand knowledge from the front lines.

These unique experiences, tailored to your organization and your industry, take place in next-gen facilities designed with style and precision to accommodate clients. Global facilities of IBM X-Force Command include:

- **IBM X-Force Command Cyber Range:** The first-ever commercial facility that immerses security staff and business leaders in a simulated environment based on a security operations center (SOC).
- **IBM X-Force Command Cyber Tactical Operations Center (C-TOC):** A unique cyber experience-on-wheels, which can be configured as a cyber range, a sterile environment for running cyber investigations, or an on-site watch floor for special security events.
- **IBM X-Force Command Executive Briefing Centers:** Meet with experienced incident responders, penetration testers, design thinking experts and IBM executives to build and hone your cybersecurity and incident response strategy.

Practice for your company's worst day

Everyone in your organization – from the SOC to the C-suite and boardroom, business units from HR to PR, and keyboard operators on the ground floor – has a role to play in responding to an attack. Is your team ready? Test the skills you have and learn the skills you need in a variety of situations based on real-life attacks.

Exercise rapid-response thinking in a pressured environment

- Respond to real-world cyberattack scenarios and injects in a realistic security operations center SOC.
- Train in gamified, high-pressure situations, led by people that have been on the front lines.
  See the impacts of untrained teams and an unprepared response plan.

Understand how security solutions work together

- Engage with multiple tools to investigate a cyber incident.
- Experience cutting-edge capabilities, such as artificial intelligence and automated incident response solutions, and how to apply them to modern investigations.
- Use real hacker tools and malware to role-play attacks in a safe and air-gapped environment.

Experience how your teams work together

- Collaborate with your cyber analysts, legal, PR, and executives during an incident.
- Review your company's playbook and crisis communication guides.
- Test non-technical teams and evaluate your media preparedness.

Stimulating challenges based on real-world scenarios

Ox Response Challenge

Collaborate in a fusion team center environment to keep your company out of the headlines. Figure out how to react as a team across the dimensions of technical, legal and public relations responses.

Learning objectives

1. Experience a cyber incident as a cross-functional business response.
2. Discover gaps in your response plan.
3. Learn technical cyber response and leadership best practices.

Who should attend

- SOC leaders: directors, team leaders
- C-level executives: CISO, CIO, CRO, COO, CEO
- Supporting teams: legal, HR, PR/Comms, Risk

Cyber Wargame

This consultative challenge is a user-driven exercise around a cyber incident. Your team is briefed, but when you enter the SOC, how your team responds is up to you. Suddenly, the first inject drops. Did you respond correctly? X-Force Command advisors will be watching and scoring against key performance indicators for precise feedback.

Learning objectives

1. Use real-world tools to discover the nature of the problem and respond to the threat.
2. Test problem-solving ability and see if you can solve the puzzle.
3. Discover how strategic and technical teams can work together.

Who should attend

- SOC leaders: directors, team leaders, managers
- Strategic and technical team members
- Supporting teams and technical analysts

OpRedEscape

To fight the bad guys, you need to think like a bad guy. Take the seat of a cyber-criminal, as you become part of a hacking crew with the goal of stealing data from a victim's network. The event culminates in a team building escape room, where you put your new skills to use. Content is customized to match the skill set in the room.

Learning objectives

1. Understand the tools attackers use to compromise a network and steal data.
2. Learn about cybercrime topics such as the dark web and crypto-ransomware.
3. Discover your "dark side" in an escape room capstone event.

Who should attend

- SOC leaders: directors, team leaders, managers
- C-level executives: CISO, CIO, CRO, COO, CEO
- Board members, investors and other leadership

An experience designed for you

- A completely immersive security experience that tests skills, process and leadership competence.
- Full- and half-day scenarios with hands-on experience and time for assessment and reflection.
- Use your own runbook if you have one.
- Tailored instruction specific to your industry and geographical location.
- Network with IBM Security incident response and managed security services leaders.

Test the skills you have. Learn the ones you need.