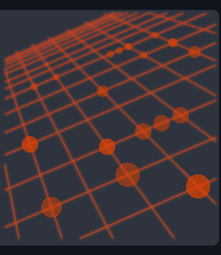
SIMSPACE

5 Critical Cyber Range Exercises

from the Experts at SimSpace

What is a cyber range?

Cyber ranges provide cybersecurity professionals with a way to practice defending against real-world attack scenarios in an isolated, highly-customizable environment. Teams can also use a cyber range to evaluate new tools and optimize their security stack.



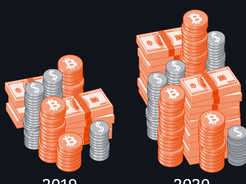
To win, you have to practice like a winner

What types of threats can be simulated in a cyber range? Here are some examples:

Mitigate ransomware

The average ransom payment increased from $115,123 in 2019 to $312,493 in 2020.[1]

- Use a cyber range to proactively test your team during a simulated version of a ransomware attack.
- Test cyber defense methods such as scanning messages and blocking IP traffic and spam.



2019 $115,123

2020 $312,493

1.6 million

more DDoS attacks were reported in 2020 than 2019.

Prevent DDoS attacks

1.6 mil more DDoS attacks were reported in 2020 than 2019.[2]

- Cyber ranges can test your security tools' ability to filter unusual traffic, block nefarious IP addresses, and so on.
- Put incident response and business continuity plans to the test in a personalized environment.

Stop malicious insiders and data breaches

Insider threats cause on average $4.61 million in damage.[3]

- Insider threat scenarios, such as abuse of user credentials and unauthorized access request, can be replicated in a range.

Insider threats cause on average **$4.61 million** in damage.

65% of survey respondents in the financial industry had at least one APT-related incident in 2016.

Protect against advanced persistent threats

Sixty-five percent of survey respondents in the financial services industry had at least one APT-related incident in 2016.[4]

- Cyber ranges allow teams to replicate complex and unpredictable attacks in a safe training environment.

Detect unauthorized network devices

An estimated 127 devices are connected to the internet for the first time each second.[5]

- Especially with the recent increase in remote work, security teams need to be extra cautious about which devices are on their network.
- You can use a cyber range to test products' ability to raise alarms about the presence of unauthorized devices or applications and abnormal user behavior.

127 devices each second

simspace.com | 1-617-237-6223 | info@simspace.com

320 Congress St. Boston, Massachusetts 02210. United States

1. Brittany Chang, "One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack," Business Insider, May 22, 2021, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5.
2. European Union Agency for Cybersecurity, "ENISA Threat Landscape 2021," October 27, 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
3. IBM Security, "Cost of a Data Breach Report 2021," July 2021, https://www.ibm.com/downloads/cas/OJDVQGRY.
4. AT&T Cybersecurity Insights, "The CEO's Guide to Navigating the Threat Landscape," 2017, https://www.business.att.com/content/dam/attbusiness/reports/vol4-threatlandscape.pdf.
5. Mark Patel, Jason Shangkuan, and Christopher Thomas, "What's new with the Internet of Things," McKinsey Digital, May 10, 2017, https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things.