

# Blue Team Exercises

Mitiga's Blue Team Exercises help organizations operating in complex cloud environments improve confidence in internal capabilities to detect, respond to, and remediate threats. Based on Mitiga's Attack Scenario Library, Blue Team Exercises help your team gain a detailed understanding of cloud security gaps. These exercises also provide detailed recommendations tailored to your toolset and environment. Customers work closely with Mitiga consultants and researchers to understand how to detect and disrupt complex cloud-based intrusions.

---

## Key Milestones in Mitiga's Blue Team Exercises

- **Kickoff.** Meeting with stakeholders to review environment, recent incidents, and cybersecurity concerns.
- **Scenario Development.** Mitiga selects and customizes attack scenarios that model your cloud security concerns. These scenarios span a variety of levels of sophistication and represent Mitiga's groundbreaking cloud security research.
- **Execution.** Mitiga serves both as the adversary and as auxiliary members of your cybersecurity team. As scenarios are deployed, Mitiga collaborates with you to validate that alerting and response capabilities meet agreed objectives.
- **Reporting.** Mitiga creates executive-level reporting that defines the scope of the exercise and provides detailed technical recommendations to address any gaps identified.

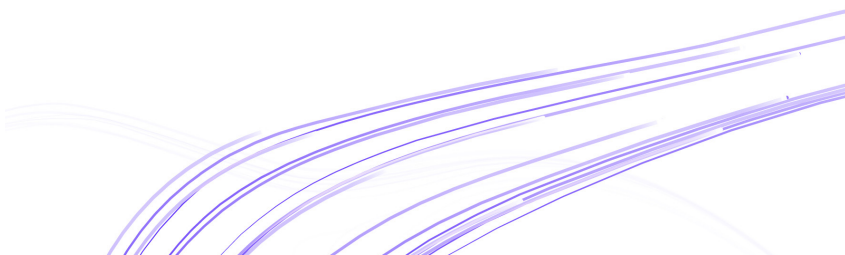
Mitiga's internal research team is central to planning and executing Blue Team Exercises. The research team combines industry-leading cybersecurity, threat intelligence, and cloud security experts to select Attack Scenarios that are specific to your environment and concerns.

Mitiga offers Blue Team Exercises to organizations with complex cloud and hybrid environments. Mitiga crafts Blue Team Exercises that reflect the perspectives of adversaries for each individual organization to discover potential exploitation and offer perspectives on insider threats to the organization. Mitiga uses in-depth knowledge of each organization's environment, personnel, and specific cybersecurity concerns to craft highly targeted and specific Attack Scenarios.

---

## Why Mitiga

Mitiga's team combines years of experience in nation-state level offensive cyber operations, a deep understanding of hackers' modes of operation and techniques, and comprehensive knowledge of cloud architecture and cloud security challenges. This enables us to provide exceptionally effective blue team exercises based on the [Homeland Security Exercise and Evaluation Program](#).



Mitiga's technology and services lower the impact of cyber breaches and optimize readiness for cloud and hybrid incidents and accelerate both response and recovery times when incidents occur. Importantly, Mitiga's readiness prioritization also increases resiliency for future incidents. Mitiga's shared-responsibility model is unique. Unlike others, who charge additional fees for incident response and recovery, Mitiga subscribers face no add-on fees.

For more information, visit [www.mitiga.io](http://www.mitiga.io) or email us at [info@mitiga.io](mailto:info@mitiga.io)