IMMERSIVELABS GUIDEPOINT® SECURITY

Put Your Crisis Team to the Test

Immersive Labs' Crisis Simulator, integrated with GuidePoint Security's professional services, gives senior management and technical teams the confidence that human assets will respond to cyber incidents more effectively.

Immersive Labs' Crisis Simulator is built to encourage resilience by upskilling humans to better withstand a modern cyber crisis. Utilizing Crisis Simulator, GuidePoint Security's certified team of cybersecurity experts drops executives, technical, and incident response teams into crisis scenarios based on the latest threats. Teams work through each crisis while measuring and continually improving response.

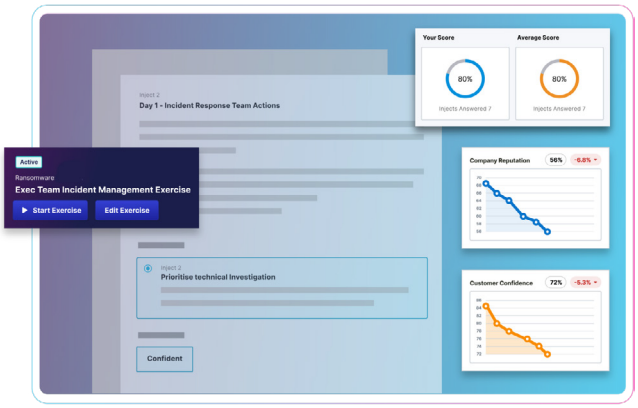
Features of Crisis Simulator

Dynamic storylines:

Incident response teams play through a fully simulated cyber crisis featuring rich, realistic narratives in straightforward business language. Decisions have a real-time impact on indicators such as share-price and reputational scores.

Relevant to you:

Simulations are customizable and continually updated using the latest attack techniques to ensure the skills learned are kept continuously fresh and relevant.



Supported by data:

Data-based insights update board members on the capabilities of incident response teams, providing confidence and clear evidence of progression.

Low organizational burden:

Being delivered through the browser makes running a crisis simulation as simple as sending a link.

Add GuidePoint's Highly Trained Experts to Your Team

Collaborate with GuidePoint's experienced security practitioners to run IR tabletop exercises and put your incident response plan through a simulated test. Choose from a list of predefined scenarios or customize a scenario to your organization's current processes, policies, and infrastructure.

In the end, you'll receive a report detailing:

- How well your team followed the existing IR plan
- How effective the plan was in addressing the simulated scenario
- Observed gaps, shortcomings, and areas for improvement
- Recommendations for improving your IR plan

GuidePoint Professional Services: Six Steps to Improving Your Security

1. GuidePoint works hand-in-hand with your team to collect information about your organization, including your current processes, policies, infrastructure, tools, and more.
2. Their Digital Forensics and Incident Response (DFIR) experts customize or develop a simulated incident for your organization in conjunction with your teams.
3. Time is scheduled to execute the simulated incident with participants, as defined in your existing incident response plan.
4. GuidePoint presents your team with a fully simulated cyber crisis that features realistic narratives in straightforward business language and observes discussions as to how your team would respond to the incident.
5. Over the course of the exercise, the facilitator provides observations, responses, and recommendations to guide your team through the incident response process.
6. GuidePoint develops a summary report of your team's handling of the incident, your IR plan's effectiveness, and recommended improvements.

Building a Tabletop Exercise That Works for You

No two organizations are the same, and neither are our tabletop exercises.
Our scenarios cover common and high-risk threats and attack patterns, including:

- Ransomware
- Supply chain attacks
- Telecommuter compromise
- Business email compromise
- Nation-state and targeted attack compromise
- Web Application exploitation
- Cloud Services compromise

IMMERSIVELABS | GUIDEPOINT® SECURITY

Cyber Resilience, Readiness, Confidence. Let's Get Started.

Contact channels@immersivelabs.com