IMMERSIVELABS

CRISIS SIM SCENARIO

INSIDER THREAT: PHARMA DRAMA

What would you do if an employee leaked your IP to a rival?

Llama Pharma is a global pharmaceutical company on the verge of something brilliant – the release of a fast-acting antidepressant that will revolutionize mental health treatment. However, a Llama representative was careless with the organization's data, which subsequently fell into the hands of its biggest rival.

In this scenario it's up to you to manage the growing crisis, track down the insider threat, and prevent the loss of potentially billions of dollars. You will also have the chance to exercise your team's technical skills in the labs that run parallel to the narrative, ensuring you are strong on both sides of the "boom".

Are you up to the challenge?

WHAT IS THIS SCENARIO ABOUT?

SECTORS	VECTORS	ACTORS	MOTIVATIONS	IMPACTS	NON-TECHNICAL SKILLS
Financial Services	Insider Threat	Organized Criminals/ Cyber	Financial	Employees	Situational Awareness
Healthcare	Ransomware	Criminal Groups	Political	Customers	Effective Leadership
Transport, Logistics & Supply Chain	DOS	Political/Social Activists	Publicity for a Cause	Operations	Rational & Intuitive Decision Making
Energy & Infrastructure	Cloud	Disgruntled Employees/Former	Personal Malice	Shareholders	Communications
Government	Vulnerability Disclosure/ Reporting	Employees/ Customers	Commercial Advantage	Financial/ Commercial	Stress Management
	Social Engineering, Fear Exploitation, Covid	Terrorist Groups	Cause Operational Delays or Disruption	Reputational	Teamwork
	Data Breach	State Actors		Legal	
	Remote Working			Regulatory	
	Electoral Fraud				
	Impersonation				
	Physical Security Breach				

This scenario focuses on an insider threat in the pharmaceutical sector, covering the impact on operations, shareholders, reputation, financial footing and regulations. It also trains many of the soft skills necessary for managing a cyber crisis and engages technical teams where desired.

WHAT SKILLS DOES THIS SCENARIO TEST?

The skills exercised in this scenario are, regardless of industry, essential to cyber crisis management at an executive level; they include situational awareness, teamwork, communication, and rational and intuitive decision making. Participants must use these skills to identify long term worst case business impacts when some certain information is unavailable.

WHAT TECHNICAL SKILLS DOES THIS SCENARIO TEST?

The scenario also engages technical teams via the linked labs, exploring various avenues of defensive security in relation to NIST's guidance on the incident response process. Below is a list of skills your cyber pros will practice in our gamified environment:

- Practical analysis of system logs
- Network activity monitoring
- Malware reverse engineering
- File enumeration in the cloud
- App vulnerability mitigation

WHY IS THIS SCENARIO IMPORTANT?

Pharma is vulnerable. The sector, which bridges the healthcare–business divide and deals extensively with data and intellectual property (IP), is a tantalizing prospect for malicious actors. It is now one of the most targeted sectors, according to **Deloitte**, with over a fifth of companies suffering at least seven attacks.

WHY SHOULD BUSINESSES CARE?

Ineffective or delayed responses to major crises (including cyber crises) can lead to significant reductions of gross earnings. By practicing and stress-testing your teams, business responses will be quicker, reducing the overall impact of the attack and allowing them to get back to 'normal' faster. The presence and reputation of companies is more prevalent now than ever, thanks to social media. Five or ten years ago, a singular fatality caused by a company's negligence may not have been disclosed or even heard about. Nowadays it spreads like wildfire. Companies need to be more socially conscious of their customers, responsibilities, and employees.