IMMERSIVELABS

CRISIS SIM SCENARIO

SUPPLY CHAIN COMPROMISE: TOO CLOSE TO THE SUN

Attacks like SUNBURST have shown that even the most secured and well-patched environments are at risk from cyber threats. Is your organization prepared?

You are the CISO of Cashmonia, a US-based banking and financial services company. A multinational business, Cashmonia has hundreds of offices and thousands of employees across the world.
Your role is to work with security professionals to secure and respond to cyber threats. You also take responsibility for communicating potential impact and actions taken to the CEO and board.

In this scenario, you'll need to make decisions that balance the risks to your organization based on available facts. You must investigate how the compromised software in your supply chain affects the security of your business, and decide what actions to take.

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				

This scenario is based on the SUNBURST attack and how it affected private businesses. It focuses on the potential financial, reputational and security impacts on an organization, forcing the player to navigate the risks involved with turning off vital network systems before all the information is available

Non-technical skills tested in this simulation include situational awareness, communication, effective leadership and rational decision making.

The scenario begins when IceNose, a cybersecurity firm, reveals it has been attacked by a sophisticated group, possibly led by a nation state. The network management technology provider LuneTyphoon provided the entry point for the attack and Cashmonia has been affected.

At the center of this scenario is a key incident: your network management software may have been compromised. The learning objective is to understand when you have enough critical information about an event to make rational decisions. The scenario also takes on a technical investigation, during which the player must complete various labs to help with findings.

WHO IS IT AIMED AT?

This scenario is aimed at executive-level crisis management teams in corporations. It will also benefit executives in any organization who are required to support their corporation's response to a major cyber breach through third party vulnerabilities.

WHY HAVE WE COVERED THIS?

The SolarWinds SUNBURST attack is one of the biggest cybersecurity crises in recent years and has affected a number of organizations across the US and UK. As the compromise came from a trusted supplier, there was nothing that the affected businesses could have done to anticipate or prevent it. Recovery and post-incident decisions are therefore at the crux of this scenario.

Stress testing teams allows them to practice their response to an incident such as this, and will help build muscle memory, resulting in a more efficient performance in the instance of a real crisis.