CLOUDGUARD

CloudGuard TableTop Exercises (TTX)

> Test the readiness and effectiveness of your organisation's Incident Response Plan with CloudGuard's simulated scenario workshops

Service Overview

Experience the effectiveness of Cybersecurity TableTop Exercises (TTX) with CloudGuard. Through simulated cyber attack scenarios, you can assess your Incident Response Plan in our collaborative "War Room" environment. Proactively identify and mitigate gaps with hands-on training tailored to your organisation's needs.

Capabilities

CloudGuard's TTX service offers a comprehensive approach to testing your incident response plans. Beginning with pre-testing consultations to develop scenarios, the service includes realistic tabletop exercises, assessing your strengths and weaknesses. With 28 scenarios, including phishing attacks, ransomware infections, and insider threats, it evaluates detection, response, and communication strategies. Feedback includes recommendations for improvement and options for support, ensuring readiness against diverse cyber threats.

Benefits

Our team of Incident Response experts are not only experienced in testing Incident Response Plans, but also in leading an Incident Response team in the height of an event. Removing the emotion of an incident and having a tested process that your organisation can rely on is only becoming more important.

- Assess and strengthen your business' Incident Response Plan
- Improve communication between stakeholders
- Develop crisis management and ensure business continuity
- Meet regulatory and requirements and compliance needs
- Be better prepared should the worst happen

CloudGuard ®

www.cloudguard.ai | hello@cloudguard.ai | +44 (0) 161 504 3313

Classification: Unrestricted
Version: cg_ttx/a/en/r1

CLOUDGUARD

ASSESS

CloudGuard TTX delivery

At CloudGuard, we're dedicated to refining and perfecting our Incident Response Simulation process to ensure your organisation is well-prepared to tackle any security challenge. Here's how we work together:

1. Info sharing

You start the process by sharing your current Incident Response Plan with us. We then schedule a kick-off call to discuss the testing details, including date, time, and location.

2. Kick-off

Before testing, we hold a 30-minute kick-off call to understand your business, customise ideal scenarios, and provide logistical guidance on who needs to attend the sessions.

3. Testing day

On the day, our consultants arrive on-site to facilitate the TTX. This comprises two distinct sessions, each lasting two hours, followed by an additional hour for debriefing and feedback.

Testing day sessions

Session One: We conduct a preparation session with your dedicated project leads, familiarising them with the format of the exercise.

Session Two: This session validates your existing Incident Response Plan in a realistic, yet controlled environment. Through discussion-based scenarios, we identify strengths and weaknesses, allowing participants to navigate through simulated security incidents.

Scenario options

As part of our service, we offer two out of a selection of 28 standard scenarios. Should you require additional scenarios, we're flexible to accommodate your needs, with pricing adjusted accordingly.

Our testing is conducted through engaging presentations and interactive Q&A sessions led by our Incident Response experts.

Comprehensive feedback

Following the TTX, we provide you with a detailed feedback document, including:

- A summary of the day's activities and key findings
- Recommended actions to improve the effectiveness of your Incident Response Plan
- Optional support from CloudGuard for remediation efforts

Who needs to attend?

We recommend that the you invite both technical and executive presence to the session.

We would use the kick-off call to discuss directly with the project leads on who would be required for Session One and Session Two.

Note: Outside of service costs, expenses associated for IR Team to travel on site will be payable

CLOUDGUARD

CloudGuard TTX attack scenarios

There are a total of 28 scenarios available to test against, built out from a core of 10 key attack types.

1. **Phishing Attack:** Deceptive emails trick employees into revealing sensitive information or credentials
2. **Ransomware Infection:** Malicious software encrypts files, demanding ransom for data decryption
3. **Data Breach:** Unauthorised access compromises sensitive customer or organisational information
4. **Insider Threat:** Disgruntled employees sabotage or steal company data or systems
5. **DDoS Attack:** Overwhelms network, rendering services inaccessible to legitimate users
6. **Supply Chain Attack:** Trusted vendor compromise leads to organisational supply chain disruption
7. **Physical Security Breach:** Unauthorised access or theft of physical assets compromises security protocols
8. **Zero-Day Exploit:** Exploits unknown software vulnerabilities, bypassing traditional security measures
9. **Social Engineering Attack:** Manipulates human psychology to gain unauthorised access to systems
10. **Regulatory Compliance Violation:** Failure to meet legal or industry standards results in penalties

About CloudGuard®

CloudGuard is a leading Managed Security Services Provider (MSSP), offering a range of services to protect organisations against evolving cyber threats. With a focus on proactive threat detection, automated response, and responsive support, CloudGuard helps businesses to navigate the complexities of the digital landscape securely.

Contact Us

CloudGuard ®

www.cloudguard.ai | hello@cloudguard.ai | +44 (0) 161 504 3313