BXC SECURITY

CIRT360 TABLETOP EXERCISE

Simulate a cyber incident and test your team's readiness before it's tested for real.

FOR **IMPACTING** BUSINESS **SOLUTIONS**

CIRT TABLETOP EXCERCISE SERVICE

BxC Security supports you in evaluating how effectively your Cyber Incident Response Team (CIRT) operates in a structured crisis scenario.
Within a controlled and realistic simulation, we assess how your organization detects, manages, and responds to a cyber incident under pressure.

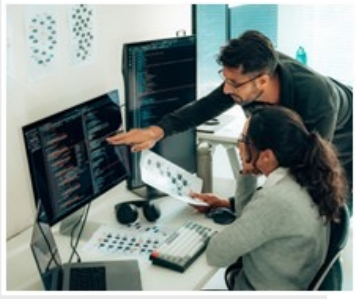
At BxC Security, our goal is to provide high-quality cybersecurity services and contribute to the resilience of our economy and society.
We focus on pragmatic and effective solutions that deliver measurable value and strengthen your organization.

Preparation

- You select a predefined incident scenario based on common threat situations
- Together, we align the exercise scope to your organizational structure
- We define the exercise flow and key discussion points based on this alignment

Execution

- We facilitate a structured tabletop exercise (4–6 hours) based on a realistic incident scenario
- Your predefined CIRT works through key decision points covering escalation, communication, and response
- We observe how your team acts under pressure



Evaluation

- We assess your team's performance based on observed decisions and actions
- We identify key gaps in communication, escalation, and role clarity
- We provide a concise summary with improvement actions and next steps

Your advantages at a glance!

- Quick and structured validation of your incident response capability
- Clear visibility of gaps in coordination and decision-making
- Practical and actionable recommendations
- Supports compliance (e.g. NIS2, ISO 27001, IEC 62443) and provides audit-ready evidence

CURIOUS TO LEARN MORE?
VISIT US AT:

https://www.bxc-security.com/

CASE STUDY

To validate its incident response capabilities, a manufacturing company with integrated IT and OT environments engaged BxC Security to conduct a structured tabletop exercise.

While a Cyber Incident Response Team (CIRT) and documented processes were already in place, the organization needed to verify whether these would function effectively in a real incident — particularly under time pressure and cross-functional coordination.
In addition, the company required documented evidence to support compliance with regulatory and standard requirements, including **NIS2 and ISO 27001**, and to demonstrate that its incident response capability had been tested in practice.

RESULTS

10+
Stakeholders involved

7+
Decision points tested

Audit-ready
Validated capability

4
Key gaps identified

Our Contribution

Preparation of the Excercise

- A predefined incident scenario is selected based on common and relevant threat situations to ensure realistic conditions
- The scope of the exercise is jointly aligned with the client, taking into account the organizational structure
- Based on this alignment, a structured exercise flow is defined, including key discussion points and decision moments to guide the session and enable a focused evaluation of the incident response capability

Execution of the Excercise

- The tabletop exercise was conducted as an interactive session, guiding participants through a realistic cyber incident scenario affecting both IT and operational environments
- Throughout the session, new information and developments were introduced to reflect evolving incident conditions and increase complexity over time
- Particular attention was given to how effectively the organization coordinated across teams, made timely decisions, and involved relevant stakeholders under pressure

Evaluation & Recommendations

- The organization's response capability was analyzed across governance, communication, and coordination
- Key gaps were identified in escalation, IT/OT alignment, and regulatory handling
- Results were documented with prioritized recommendations and clear improvement actions

OUR OFFER- remote delivery

***on-site pricing on request**

We offer a structured and pragmatic service that enables you to validate your incident response capability under realistic conditions.

The objective is to provide clarity on how your Cyber Incident Response Team performs in practice and to identify concrete improvement areas with minimal preparation effort on your side.

CIRT TABLETOP EXCERCISE

Our structured tabletop exercise provides a fast and efficient way to test your Cyber Incident Response Team in a realistic scenario.

Within a focused session, your team works through a predefined incident, allowing you to validate decision-making, coordination, and communication under pressure.

We bring the scenario, facilitation, and evaluation methodology — you bring your team and organizational context.

Price: 10.000 Euro

What we need

- List of relevant stakeholders (e.g. IT, security, operations, management)
- Basic overview of your incident response setup
- Availability for a 4–6 hour session
- High-level information about your IT/OT environment

What you get

- Facilitated tabletop exercise
- Realistic predefined incident scenario
- Structured assessment of response capability
- Identification of key gaps and weaknesses
- Concise report with recommendations and next steps

BXC SECURITY

info@bxc-security.com

+49 811 128 807 43

Foehrenweg 1
85399 Hallbergmoos
Germany

FOR **IMPACTING**
BUSINESS **SOLUTIONS**