KUDELSKI SECURITY

PARTNER PROGRAM

INCIDENT RESPONSE PLAN DEVELOPMENT

Prepare and train for the security events most likely to impact your business

Does your organization have a well-defined plan to contain and mitigate a security incident? Are your teams properly trained to carry out the steps effectively?

The development of a comprehensive Incident Response Plan is a crucial step in addressing these concerns and building an effective overall Incident Response Program.

Kudelski Security works with you to deliver a cyber resilience policy and playbooks which integrate seamlessly with your people and processes and include technical and strategic guidance on effectively identifying, containing, and neutralizing suspected incidents. These documents will align your Incident Response Program to Kudelski Security's Incident Response Framework.

APPROACH

- Conduct an onsite workshop where we customize our Incident Response Framework to your business context.
- Develop or improve your Incident Response Plan by incorporating your existing internal procedures and personnel feedback with our cybersecurity expertise. Identify how to effectively identify, contain, and respond to the most likely cyber incidents facing your organization.

BENEFITS

- Reduce the impact of a data breach and cost to your business with an effective plan and experienced team.
- Define response processes and optimize the people, processes, and technologies involved.
- Eliminate delays in effective containment and remediation due to lack of clear lines of responsibility and multi-stakeholder ownership
- Align your cyber resilience approach with your corporate strategy.

SERVICE OPTIONS

1

100+
EMPLOYEES

SCOPE

Access to
1 business unit

Up to
2 days onsite
conducting at least
8 interviews

Review up to
4 relevant internal documents

Provide at least
2 Cyber Resilience Playbooks

2

250+
EMPLOYEES

SCOPE

Access to
3 business units

Up to
3 days onsite
conducting at least
12 interviews

Review up to
6 relevant internal documents

Provide at least
5 Cyber Resilience Playbooks and Threat Model Report

3

350+
EMPLOYEES

SCOPE

Access to
6 business units

Up to
5 days onsite
conducting at least
20 interviews

Review up to
12 relevant internal documents

Provide at least
10 Cyber Resilience Playbooks and Threat Model Report

KEY DELIVERABLES

- Cyber Resilience Policy – the core framework for the Incident Response process.
- Cyber Resilience Playbook – an actionable plan to swift Incident Response.
- Cyber Playcards that provide a consolidated, single pane view of steps in the Incident Response process.
- Training for Primary and Secondary Incident Response support teams.
- Threat Model Report can also be provided.This report will give you a systematic analysis of the controls or defenses needed to deter an attacker based on an attacker's profile, your most valuable assets, and the probable attack vectors.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY