CYBER RESILIENCE PROGRAM DEVELOPMENT

Advisory Services

Prepare and train for the security events most likely to impact your business in order to strengthen your incident response readiness.

No matter the size or industry, no organization is immune to attack. Yet many organizations lack a clearly defined plan to contain and mitigate a security incident when it does occur. The first time you test your incident response capabilities should not be during a live event. Preparation and practice are key to limiting the impact and getting back to business as usual.

The Kudelski Security Cyber Resilience Program Development suite of services helps organizations achieve a state of response preparedness for emerging threats. Our cyber advisors will provide technical and strategic guidance across all disciplines of the incident response process to help clients effectively respond to and contain incidents, and ultimately build up their cyber resilience.

Key Outcomes

- Develop and communicate a clear plan of action for response that aligns with corporate objectives
- Train and test your team's ability to respond to business-relevant threats in a controlled environment
- Reduce the time to detect threats and resolve critical security incidents
- Minimize potential disruptions to business due to a security breach
- Get executive-level justification for incident response investments
- Gain confidence in your organization's state of preparedness for a cybersecurity attack

Kudelski Security has developed three offerings to improve resiliency against cyber threats.

ASSESS
Cyber Resilience Readiness Review

PREPARE
Cyber Resilience Policy & Playbook

VALIDATE
Tabletop & Threat Simulation

The Kudelski Security Advantage

We leverage our Secure Blueprint approach to build mature and effective IR programs.

A team of principal-level consultants with expertise across industries and IR disciplines.

We seek to understand your business and capabilities to deliver custom solutions for IR.

Our Approach to Cyber Resilience

Assess

Readiness is crucial for effective security incident response. A proactive approach can significantly decrease response time, costs, and the overall impact of a security breach.

Prepare

The Cyber Resilience Policy & Playbook engagement is an opportunity to clearly define response processes and optimize the people, processes, and technologies involved.

Validate

Testing the incident response program, processes, and teams enables clients to observe how their business would respond to a real-world cyber attack.

What We Deliver

Cyber Resilience Program Development is comprised of three strategic services to help you assess, prepare, and validate your cyber resiliency.

Assess – Cyber Resilience Readiness Review

The Cyber Resilience Readiness Review will provide strategic guidance on effectively detecting, containing, eradicating, and remediating suspected incidents and limiting their impact on the business. Available in an executive workshop format, our advisors will collaborate with leadership teams to evaluate current capabilities and gaps in incident response processes. We will also identify key building blocks for your risk mitigation strategy and develop a smart roadmap driven by business context and threat landscape to enable effective incident response operations.

Engagement Deliverables: *A Cyber Resilience Incident Response Plan, Executive-Level Summary of Findings, Technical Report of Findings & Recommendations, Incident Response Leadership Training*

Prepare – Cyber Resilience Policy & Playbook Development

During an onsite workshop, our advisors will use our Incident Response Framework – adapted to your context and existing threat landscape – to develop or update your emergency response plan. The plan will also incorporate the personnel and procedures needed to effectively identify, contain, and respond to the most likely cyber attacks as well as the attack vectors that introduce the most risk.

Engagement Deliverables: *Cyber Resilience Policy – the core framework for the Incident Response process, Cyber Resilience Playbook – an actionable guide to swift Incident Response, Cyber Playcards – consolidated, single-pane view of steps in the IR process, Training for Primary/Secondary IR Support Teams*

Validate – Tabletop & Threat Simulation

Kudelski Security's Tabletop & Threat Simulations use lessons learned from real-world response scenarios to test your organization's ability to respond to an attack. Interactive sessions are tailored to your own threat model and use progressive stages of simulated attack to evaluate both the executive and technical teams' ability to respond during a high-impact security breach.

Engagement Deliverables: *A simulation crafted according to client's needs (including executive response exercise, task-based exercises for internal incident response, and war games for APT identification), Executive-level Summary of Findings, Technical Report of Findings & Recommendations*

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