

# INCIDENT RESPONSE & CYBER RESILIENCE

## Advisory Services



Implement programs to build resilience against cyber attacks and receive emergency support in detecting, containing, and mitigating attacks.

As threats become more sophisticated and pervasive, organizations must improve their resilience through better preparation. They need to be sure they can remediate as swiftly as possible – containing the attack, mitigating attacker access – and getting back to business as soon as possible.

No organization will ever be completely immune to attacks, but Kudelski Security can help CISOs proactively build strategies for preventing and responding to them. We leverage our Secure Blueprint approach to measure the organization's current response readiness and establish a plan to achieve the desired state. In addition, team training, threat simulations and communication plans ensure all relevant parties – from the executive to the technical level – understand and support the response plan. In the event of a breach, CISOs can also call on our team of world-class cyber-response advisors to help identify, contain and remediate attacks.

## Incident Response & Cyber Resilience - Advisory Services

### Key Outcomes

- A common understanding of the organization's current and desired state of readiness
- Assurance that your team is prepared to respond in the event of a breach
- Peace of mind, with a trusted partner on standby with resources and capabilities to respond the moment a breach occurs
- Priority access and SLA assurance from our Global Incident Response team
- Actionable reporting with a direct correlation to the overall strategic program



### The Kudelski Security Advantage



Kudelski Security's proprietary Secure Blueprint approach is leveraged to build mature and highly functional incident response programs



A team of principal-level consultants with experience in different industry verticals



Expertise in enterprise digital forensics and incident response, with world-class labs and analysis capabilities

## How We Engage

Incident Response & Cyber Resilience Services can be delivered ad-hoc or through a multi-year subscription that includes a retained incident response team and access to the catalog of other Advisory Services.

### Identify Services

An account manager will help identify the service that best fits your needs – readiness review, training and testing, threat hunting, retained incident response or emergency incident response.

### Define Scope & Goals

A Kudelski Security advisor will meet with you to define the scope and specific goals for the engagement. Project planning proceeds according to the requested service and desired outcomes.

### Establish the Team

For response services, you will have access to a dedicated consulting team, typically made up of four or more members:

- Managing Director – Incident Management & Coordination with Counsel
- Principal-lead Investigator and Primary POC
- Senior Consultant-investigator
- SME/Consultant-investigator

Kudelski Security has long-standing relationships with law enforcement and premier law firms as well as key forensic and response vendors.

## Incident Response & Cyber Resilience

Crossing disciplines of cyber law, forensics, technology, privacy and cyber assurance, our Incident Response & Cyber Resilience advisors guide organizations in building proactive strategies against emerging threats, and help them reach their desired state of preparedness.

Our advisors are skilled in incident response, leveraging people, process and technology to deliver rapid breach containment and risk mitigation.

### • Cyber Resilience Program Development

- **Cyber Resilience Readiness Review:** Kudelski Security leverages its Secure Blueprint approach to measure an organization against a comprehensive set of disciplines designed to mature your incident response program. Available in an executive workshop format, our advisors will collaborate with leadership teams to evaluate current response readiness and develop a strategic roadmap driven by business context and threats, which enable effective incident response operations.
- **Cyber Resilience Policy & Playbooks:** Our advisors will use our Incident Response Framework, adapted to your context, to develop or update your emergency response plan, incorporating the personnel and procedures needed to effectively identify, contain, and respond to the most likely cyber incidents.
- **Tabletop & Threat Simulation:** Our advisors use lessons learned from the field 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.
- **Emergency Response & On-demand Retainers:** From initial breach discovery to expert testimony, our experienced team of advisors work alongside CISOs to provide guidance through the incident response lifecycle and outline mitigation plans to reduce reoccurrence. On-demand retainers accelerate the time-to-action in the event of a breach, resulting in faster containment and reduced business impact.
- **Compromise Assessment:** Our threat analysts examine your computing environment for malicious activity to uncover attack history and breach exposure, enabling you to identify or confirm compromised data and initiate proper response. Most importantly, the threat hunting team will provide steps for containment and recommendations for future safeguarding of your assets.

Incident Response and Cyber Resilience is one of four service pillars under Kudelski Security Advisory Services. The other three pillars of which Kudelski Security has deep knowledge and experience are Strategy & Governance, Threat, Vulnerability & Risk Management, and Strategic Cyber Staffing.

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](mailto:Info@kudelskisecurity.com) | [www.kudelskisecurity.com](http://www.kudelskisecurity.com)

